On Nichols algebras associated to simple racks

N. Andruskiewitsch, F. Fantino, G. A. García, L. Vendramin

Dedicado a Matías Graña

Abstract. This is a report on the present state of the problem of determining the dimension of the Nichols algebra associated to a rack and a cocycle. This is relevant for the classification of finite-dimensional complex pointed Hopf algebras whose group of group-likes is non-abelian. We deal mainly with simple racks. We recall the notion of rack of type D, collect the known lists of simple racks of type D and include preliminary results for the open cases. This notion is important because the Nichols algebra associated to a rack of type D and any cocycle has infinite dimension. For those racks not of type D, the computation of the cohomology groups is needed. We discuss some techniques for this problem and compute explicitly the cohomology groups corresponding to some conjugacy classes in symmetric or alternating groups of low order.

1. Introduction

The problem of classifying finite-dimensional pointed Hopf algebras over non-abelian finite groups reduces in many cases to a question on conjugacy classes. In this introduction we give a historical account and place the problem in the overall picture.

1.1. We briefly recall the lifting method for the classification of pointed Hopf algebras, see Subsection 2.2 for unexplained terminology and [**AS2**] for a full exposition. Let H be a Hopf algebra with bijective antipode and assume that the coradical $H_0 = \sum_{C \text{ simple subcoalgebra of } H} C$ is a Hopf subalgebra of H. Consider the coradical filtration of H:

$$H_0 \subset H_1 \subset \cdots \subset H = \bigcup_{n\geq 0} H_n,$$

where $H_{i+1} = \{x \in H : \Delta(x) \in H_i \otimes H + H \otimes H_0\}$. Then the associated graded coalgebra $\operatorname{gr} H$ has a decomposition $\operatorname{gr} H \simeq R\# H_0$, where R is an algebra with

2010 *Mathematics Subject Classification.* 16T05; 17B37.

This work was partially supported by ANPCyT-Foncyt, CONICET, Ministerio de Ciencia y Tecnología (Córdoba), Secyt-UNC and Secyt-UBA.

some special properties and # stands for a kind of semidirect product (technically, a Radford biproduct or bosonization; the underlying vector space is $R \otimes H_0$). The algebra R, more precisely, is a Hopf algebra in the braided tensor category of Yetter-Drinfeld modules over H_0, see Subsection 2.2, and inherits the grading of $\operatorname{gr} H$: $R = \oplus_{n \geq 0} R^n$. If $V = R^1$, then the subalgebra of R generated by V is isomorphic to the Nichols algebra $\mathfrak{B}(V)$, that is completely determined by the Yetter-Drinfeld module V.

Let us fix a semisimple Hopf algebra A. One of the fundamental steps of the lifting method to classify finite-dimensional Hopf algebras H with $H_0 \simeq A$ is to address the following question, see [**A**]:

Question. *Determine the Yetter-Drinfeld modules V over A such that the dimension of $\mathfrak{B}(V)$ is finite, and if so, give an efficient set of relations of $\mathfrak{B}(V)$.*

An important observation is that the Nichols algebra $\mathfrak{B}(V)$, as algebra and coalgebra, is completely determined just by the braiding $c : V \otimes V \to V \otimes V$. Therefore, it is convenient to consider classes of braided vector spaces (V, c) depending on the class of semisimple Hopf algebras we are considering.

1.2. A Hopf algebra H is pointed if H_0 is isomorphic to the group algebra $\mathbb{C}G$, where G is the group of grouplikes of H. Let us consider first the case when G is abelian. A braided vector space (V, c) is of diagonal type if V has a basis $(v_i)_{1 \leq i \leq n}$ such that $c(v_i \otimes v_j) = q_{ij} v_j \otimes v_i$, where the q_{ij}'s are non-zero scalars [**AS1**]. The class of braided vector spaces of diagonal type corresponds to the class of pointed Hopf algebras with G abelian (and finite). A remarkable result is the complete list of all braided vector spaces of diagonal type with finite-dimensional Nichols algebra [**H2**]; the basic tool in the proof of this result is the Weyl groupoid [**H1**]. The classification of all finite-dimensional pointed Hopf algebras with G abelian and order of G coprime with 210 was obtained in [**AS3**], relying crucially on [**AS1, H2**]. Notice however that the article [**H2**] does not contain the efficient set of relations for finite-dimensional Nichols algebras of diagonal type; so far, this is available for the special classes of braided vector spaces of Cartan type [**AS1**] and more generally of standard type [**Ang**].

1.3. Let us now turn to the case when H is pointed with G non-abelian and mention some antecedents.

- ⋄ The first genuine examples of finite-dimensional pointed Hopf algebras with non-abelian group appeared in [**MS, FK**], as bosonizations of Nichols algebras related to the transpositions in $\mathbb{S}_3$ and $\mathbb{S}_4$, see Subsection 6.2. The analogous quadratic algebra over $\mathbb{S}_5$ was computed by Roos with a computer and proved to be a Nichols algebra in [**G2**].
- ⋄ In [**G1**], Graña identified the class of braided vector spaces corresponding to pointed Hopf algebras with non-abelian group as those constructed from racks and cocycles. He also computed in [**G2**] several finite-dimensional Nichols algebras with the help of computer programs.
- ⋄ In [**G1**], Graña also suggested to look at braided vector subspaces to decide that a Nichols algebra has infinite dimension. After [**H2**], this idea

was implemented in several papers, by looking at abelian subracks. See [**AF1, AF2, AFZ, AZ, F, FGV1, FGV2**].

- ◇ The construction of the Weyl groupoid for braided vector spaces of diagonal type in [**H1**] was extended to braided vector spaces arising from semisimple Yetter-Drinfeld modules in [**AHS**]. This allowed to consider braided vector subspaces associated to non-abelian subracks [**AF3**]. A further study of the Weyl groupoid in [**AHS**] was undertaken in [**HS**]. An important consequence of one of the results in [**HS**] is the notion of rack of type D [**AFGV1**].

1.4. We shall explain in detail the notion of rack of type D in Subsection 2.4, but we try now to give a glimpse. As we explain in Subsection 2.2, our goal is to determine if the Nichols algebra $\mathfrak{B}(\mathcal{O}, \rho)$ related to a conjugacy class $\mathcal{O}$ in a finite group G and a representation ρ of the centralizer is finite-dimensional. We say that the conjugacy class $\mathcal{O}$ is *of type D* if there exist $r, s \in \mathcal{O}$ such that

(1) $(rs)^2 \neq (sr)^2$,
(2) r is not conjugated to s in the subgroup of G generated by r, s.

Then $\dim \mathfrak{B}(\mathcal{O}, \rho) = \infty$ *for any* ρ; furthermore this will happen for any group G' containing $\mathcal{O}$ as a conjugacy class (that is, as a subrack). By reasons exposed in Subsection 2.4, we focus on the following case.

Question 1. *Determine all simple racks of type D.*

The classification of finite simple racks is known, see Subsection 2.5; the list consists of conjugacy classes in groups of 3 types. In other words, we need to check, for each conjugacy class in the list of simple racks, whether there exist r, s satisfying (1) and (2) above. The main purpose of this paper is to report the actual status of this purely group-theoretical question, that is succinctly as follows.

- ◇ [**AFGV1**] The conjugacy classes in the alternating and symmetric groups, $\mathbb{A}_m$ and $\mathbb{S}_m$, are of type D, except for a short list of exceptions listed in Theorems 5.1 and 6.1; for some of these exceptions, we know that they are not of type D, see Remark 4.2 in *loc. cit.*
- ◇ [**AFGV2**] The conjugacy classes in the sporadic groups are of type D, except for a short list of exceptions listed in Theorems 5.2; for some of these, we know that they are not of type D, see Table 2. The verification was done with the help of GAP, see [**AFGV3**].
- ◇ [**FV**] Twisted conjugacy classes of sporadic groups are also mostly of type D, except for a short list of exceptions, see Theorem 6.2.
- ◇ [**AFGaV**] Some techniques to deal with twisted homogenous racks were found; so far, most of the examples dealt with are of type D.
- ◇ We include in Subsection 5.3 some preliminary results on conjugacy classes on simple groups of Lie type; again, most of the examples are of type D.
- ◇ The simple affine racks does not seem to be of type D.

What happens beyond type D? As we see by now, there are roughly two large classes of simple racks, one formed by the affine ones and the conjugacy class of transpositions in $\mathbb{S}_m$, and the rest. For this second class, our project is to finish

the determination of those of type D and attack the remaining ones as explained in page 8. That is, to compute the pointed sets of cocycles of degree n and then try to discard the corresponding braided vector spaces by abelian techniques. The first class is not tractable by the strategy of subracks. We should also mention the recent paper [**GHV**] with a different approach.

1.5. The paper is organized as follows. We discuss Nichols algebras, racks, cocycles, the criterion of type D, the classification of finite simple racks and the strategy of subracks in Section 2. Section 3 contains some techniques for the computation of cocycles. In the next sections we list explicitly the simple racks that are known to be of type D. In Section 8 we illustrate the consequences of these results to the classification of pointed Hopf algebras. In Appendix A, we list all known examples of finite-dimensional Nichols algebras associated to racks and cocycles; in Appendix B, we put together some questions scattered along the text.

This survey contains also a few new concepts and results, among them: the computation of the enveloping group of the rack of transpositions in $\mathbb{S}_m$, see Proposition 3.2; the twisting operation for cocycles on racks, see Subsection 3.4; the calculation of some cohomology groups using the program RiG, see Subsection 3.3; some preliminary discussions on conjugacy classes of type D in finite groups of Lie type, see Subsection 5.3.

2. Preliminaries

Conventions. $\mathbb{N} = \{1, 2, 3, \dots\}$; $\mathbb{S}_X := \{f : X \to X \text{ bijective}\}$; if $m \in \mathbb{N}$, then $\mathbb{G}_m$ is the group of m-th roots of 1 in $\mathbb{C}$.

2.1. Racks.

We briefly recall the basics of racks; see [**AG**] for more information and references. A *rack* is a pair $(X, \triangleright)$ where X is a non-empty set and $\triangleright : X \times X \to X$ is an operation such that

$$\text{the map } \varphi_x = x \triangleright \underline{\quad} \text{ is bijective for any } x \in X, \quad \text{and} \tag{1}$$

$$x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (x \triangleright z) \text{ for all } x, y, z \in X. \tag{2}$$

A group G is a rack with $x \triangleright y = xyx^{-1}$, $x, y \in G$; if $X \subset G$ is stable under conjugation by G, that is a union of conjugacy classes, then it is a subrack of G. The main idea behind the consideration of racks is to keep track just of the conjugation of a group. Morphisms of racks and subracks are defined as usual. For instance, $\varphi : X \to \mathbb{S}_X$, $x \mapsto \varphi_x$, is a morphism of racks, for any rack X. Any rack X considered here satisfies the conditions

$$x \triangleright x = x, \tag{3}$$

$$x \triangleright y = y \implies y \triangleright x = x, \tag{4}$$

for any $x, y \in X$. This is technically a *crossed set*, but we shall simply say a rack. So, we rule out, for example, the permutation rack (X, σ), where $\sigma \in \mathbb{S}_X$ and $\varphi_x = \sigma$ for all x.

The rack with just one element is called *trivial*.

We shall consider some special classes of racks that we describe now.

Affine racks. If A is an abelian group and $T \in \operatorname{Aut}(A)$, then A is a rack with $x \triangleright y = (1 - T)x + Ty$. This is called an *affine rack* and denoted $\mathsf{Q}_{A,T}$.

Twisted conjugacy classes. Let G be a finite group and $u \in \mathrm{Aut}(G)$; G acts on itself by $x \rightharpoonup_u y = x\, y\, u(x^{-1})$, $x, y \in G$. The orbit $\mathcal{O}_x^{G,u}$ of $x \in G$ by this action is a rack with operation

$$y \triangleright_u z = y\, u(z\, y^{-1}), \quad y, z \in \mathcal{O}_x^{G,u}. \tag{5}$$

We shall say that $\mathcal{O}_x^{G,u}$ is a *twisted conjugacy class* of type (G, u).

Notation.

- $\mathcal{T}$ = any of the conjugacy classes of 3-cycles in $\mathbb{A}_4$ (the tetrahedral rack).
- $\mathsf{Q}_{A,T}$ = affine rack associated to an abelian group A and $T \in \mathrm{Aut}(A)$.
- $\mathcal{D}_n$ = class of involutions in the dihedral group of order $2n$, n odd.
- $\mathcal{O}_j^m$ = conjugacy class of j-cycles in $\mathbb{S}_m$.

We need some terminology on racks.

- A rack X is *decomposable* if it can expressed as a disjoint union of subracks $X = X_1 \coprod X_2$. Otherwise, X is *indecomposable*.
- A rack X is said to be *simple* iff $\operatorname{card} X > 1$ and for any surjective morphism of racks $\pi : X \to Y$, either π is a bijection or $\operatorname{card} Y = 1$.
- If X is a rack and $j \in \mathbb{Z}$, then $X^{[j]}$ is the rack with the same set X and multiplication $\triangleright^j$ given by $x \triangleright^j y = \varphi_x^j(y)$, $x, y \in X$.

2.2. Nichols algebras.

Nichols algebras play a crucial role in the classification of Hopf algebras, see [**AS2**] or a brief account in Section 8 below. Let $n \geq 2$ be an integer. We start by reminding the well-known presentations by generators and relations of the braid group $\mathbb{B}_n$ and the symmetric group $\mathbb{S}_n$:

$$\mathbb{B}_n = \langle (\sigma_i)_{1 \leq i \leq n-1} | \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j,\ |i-j| = 1; \quad \sigma_i \sigma_j = \sigma_j \sigma_i,\ |i-j| > 1 \rangle$$

$$\mathbb{S}_n = \langle (s_i)_{1 \leq i \leq n-1} | s_i s_j s_i = s_j s_i s_j,\ |i-j| = 1; \quad s_i s_j = s_j s_i,\ |i-j| > 1; \quad s_i^2 = e \rangle,$$

indices in the relations going over all possible i, j. There is a canonical projection $\pi : \mathbb{B}_n \to \mathbb{S}_n$, that admits a so-called Matsumoto section $M : \mathbb{S}_n \to \mathbb{B}_n$; this is not a morphism of groups, and it is defined by $M(s_i) = \sigma_i$, $1 \leq i \leq n-1$, and $M(st) = M(s)M(t)$, for any $s, t \in \mathbb{S}_n$ such that $l(st) = l(s) + l(t)$, l being the length function.

Let V be a vector space and $c \in \mathbf{GL}(V \otimes V)$. Recall that c fulfills the braid equation if $(c \otimes \mathrm{id})(\mathrm{id} \otimes c)(c \otimes \mathrm{id}) = (\mathrm{id} \otimes c)(c \otimes \mathrm{id})(\mathrm{id} \otimes c)$. In this case, we say that (V, c) is a *braided vector space* and that c is a *braiding*. Since c satisfies the braid equation, it induces a representation of the braid group $\mathbb{B}_n$, $\rho_n : \mathbb{B}_n \to \mathbf{GL}(V^{\otimes n})$, for each $n \geq 2$. Explicitly, $\rho_n(\sigma_i) = \mathrm{id}_{V^{\otimes(i-1)}} \otimes c \otimes \mathrm{id}_{V^{\otimes(n-i-1)}}$, $1 \leq i \leq n-1$. Let

$$Q_n = \sum_{\sigma \in \mathbb{S}_n} \rho_n(M(\sigma)) \in End(V^{\otimes n}). \tag{6}$$

Then the *Nichols algebra* $\mathfrak{B}(V)$ is the quotient of the tensor algebra $T(V)$ by $\oplus_{n \geq 2} \ker Q_n$, in fact a 2-sided ideal of $T(V)$. If $c = \tau$ is the usual switch, then $\mathfrak{B}(V)$ is just the symmetric algebra of V; if $c = -\tau$, then $\mathfrak{B}(V)$ is the exterior algebra of V. But the computation of the Nichols algebra of an arbitrary braided vector space is a delicate issue. We are interested in the Nichols algebras of the braided vector spaces arising from Yetter-Drinfeld modules[1].

[1] Any braided vector space with *rigid* braiding arises as a Yetter-Drinfeld module [**Tk**].

A *Yetter-Drinfeld module* over a Hopf algebra H with bijective antipode $\mathcal{S}$ is a left H-module M and simultaneously a left H-comodule, with coaction $\lambda : M \to H \otimes M$ compatible with the action in the sense that $\lambda(h \cdot x) = h_{(1)}x_{(-1)}\mathcal{S}(h_{(3)}) \otimes h_{(2)} \cdot x_{(0)}$, for any $h \in H$, $x \in M$. Here $\lambda(x) = x_{(-1)} \otimes x_{(0)}$, in Heyneman-Sweedler notation. A Yetter-Drinfeld module M is a braided vector space with $c(m \otimes n) = m_{(-1)} \cdot n \otimes m_{(0)}$, $m, n \in M$. We shall see in Section 8 how Nichols algebras of Yetter-Drinfeld modules enter into the classification of Hopf algebras. In this paper, we are interested in the case when $H = \mathbb{C}G$ is the group algebra of a finite group G. In this setting, a Yetter-Drinfeld module over H is a left G-module M that bears also a G-gradation $M = \oplus_{g\in G} M_g$, compatibility meaning that $h \cdot M_g = M_{hgh^{-1}}$ for all $h, g \in G$; the braiding is $c(m \otimes n) = g \cdot n \otimes m$, $m \in M_g$, $n \in M$.

Now a braided vector space may be realized as a Yetter-Drinfeld module over many different groups and in many different ways. It is natural to look for a description of the class of braided vector spaces that actually arise as Yetter-Drinfeld modules over some finite group and to study them by their own. If G is a finite group, then any Yetter-Drinfeld module over the group algebra $\mathbb{C}G$ is semisimple. Furthermore, it is well-known the set of isomorphism classes of irreducible Yetter-Drinfeld modules over $\mathbb{C}G$ is parameterized by pairs $(\mathcal{O}, \rho)$, where $\mathcal{O}$ is a conjugacy class of G and ρ is an irreducible representation of the centralizer of a fixed point in $\mathcal{O}$. M. Graña observed that the class of braided vector spaces arising from Yetter-Drinfeld modules over finite groups is described using racks and cocycles, see [**G1**] and also [**AG**, Th. 4.14].

2.3. Nichols algebras associated to racks and cocycles.

We are focused in this paper on Nichols algebras associated to braided vector spaces build from racks and cocycles. We start by describing the cocycles associated to racks. Let X be a rack and $n \in \mathbb{N}$. A map $\mathbf{q} : X \times X \to \mathbf{GL}(n, \mathbb{C})$ is a *2-cocycle* of degree n if

$$\mathbf{q}_{x,y\triangleright z}\mathbf{q}_{y,z} = \mathbf{q}_{x\triangleright y,x\triangleright z}\mathbf{q}_{x,z},$$

for all $x, y, z \in X$. Let $\mathbf{q}$ be a 2-cocycle of degree n, $V = \mathbb{C}X \otimes \mathbb{C}^n$, where $\mathbb{C}X$ is the vector space with basis e_x, for $x \in X$. We denote $e_x v := e_x \otimes v$. Consider the linear isomorphism $c^{\mathbf{q}} : V \otimes V \to V \otimes V$,

$$c^{\mathbf{q}}(e_x v \otimes e_y w) = e_{x\triangleright y}\mathbf{q}_{x,y}(w) \otimes e_x v, \tag{7}$$

$x, y \in X$, $v, w \in \mathbb{C}^n$. Then $c^{\mathbf{q}}$ is a solution of the braid equation:

$$(c^{\mathbf{q}} \otimes \mathrm{id})(\mathrm{id} \otimes c^{\mathbf{q}})(c^{\mathbf{q}} \otimes \mathrm{id}) = (\mathrm{id} \otimes c^{\mathbf{q}})(c^{\mathbf{q}} \otimes \mathrm{id})(\mathrm{id} \otimes c^{\mathbf{q}}).$$

Example 2.1. Let X be a finite rack and $\mathbf{q}$ a 2-cocycle. The dual braided vector space of $(\mathbb{C}X \otimes \mathbb{C}^n, c^{\mathbf{q}})$ is isomorphic to $(\mathbb{C}X^{[-1]} \otimes \mathbb{C}^n, c^{\widehat{\mathbf{q}}})$ where $\widehat{\mathbf{q}}_{x,y} = \mathbf{q}_{x,x\triangleright^{-1}y}$, $x, y \in X^{[-1]}$. See Subsection 2.1 for $X^{[-1]}$.

The Nichols algebra associated to $c^{\mathbf{q}}$ is denoted $\mathfrak{B}(X, \mathbf{q})$.

We need to consider only 2-cocycles (or simply cocycles, for short) with some specific properties.

- A cocycle $\mathbf{q}$ is *finite* if its image generates a finite subgroup of $\mathbf{GL}(n, \mathbb{C})$.
- A cocycle $\mathbf{q}$ is *faithful* if the morphism of racks $g : X \to \mathbf{GL}(V)$ defined by $g_x(e_y w) = e_{x\triangleright y}\mathbf{q}_{x,y}(w)$, $x, y \in X$, $w \in V$, is injective.

We denote by $Z^2(X, \mathbf{GL}(n, \mathbb{C}))$ the set of all finite faithful 2-cocycles of degree n. Let $\mathbf{q} \in Z^2(X, \mathbf{GL}(n, \mathbb{C}))$ and $\gamma : X \to \mathbf{GL}(n, \mathbb{C})$ a map whose image generates a finite subgroup. Define $\widetilde{\mathbf{q}} : X \times X \to \mathbf{GL}(n, \mathbb{C})$

$$\widetilde{\mathbf{q}}_{ij} = (\gamma_{i \triangleright j})^{-1} \mathbf{q}_{ij} \gamma_j. \tag{8}$$

Then $\widetilde{\mathbf{q}}$ is also a finite faithful cocycle and "$\mathbf{q} \sim \widetilde{\mathbf{q}}$ iff they are related by (8) for some γ" defines an equivalence relation. We set

$$H^2(X, \mathbf{GL}(n, \mathbb{C})) = Z^2(X, \mathbf{GL}(n, \mathbb{C})) / \sim . \tag{9}$$

If $\mathbf{q} \sim \widetilde{\mathbf{q}}$, then the Nichols algebras $\mathfrak{B}(X, \mathbf{q})$ and $\mathfrak{B}(X, \widetilde{\mathbf{q}})$ are isomorphic as braided Hopf algebras in the sense of [**Tk**], see [**AG**, Th. 4.14]. The converse is not true, see [**G1**].

The main question we want to solve is the following.

Question 2. *For any finite indecomposable rack X, for any $n \in \mathbb{N}$, and for any $\mathbf{q} \in H^2(X, \mathbf{GL}(n, \mathbb{C}))$, determine if $\dim \mathfrak{B}(X, \mathbf{q}) < \infty$.*

Definition 2.2. An indecomposable finite rack X *collapses at n* if for any finite faithful cocycle $\mathbf{q}$ of degree n, $\dim \mathfrak{B}(X, \mathbf{q}) = \infty$; X *collapses* if it collapses at n for any $n \in \mathbb{N}$.

The first idea that comes to the mind is one would need to compute the group $H^2(X, \mathbf{GL}(n, \mathbb{C}))$ for any n. We shall see that in many cases this is actually not necessary.

Question 3. *If X collapses at 1, does necessarily X collapse?*

Even partial answers to Question 3 would be very interesting.

2.4. Racks of type D.

We now turn to a setting where the calculation of the cocycles is not needed.

Definition 2.3. Let $(X, \triangleright)$ be a rack. We say that X is *of type D* if there exists a decomposable subrack $Y = R \coprod S$ of X such that

$$r \triangleright (s \triangleright (r \triangleright s)) \neq s, \quad \text{for some } r \in R, s \in S. \tag{10}$$

The following important result is a consequence of [**HS**, Th. 8.6], proved using the main result of [**AHS**].

Theorem 2.4. [**AFGV1**, Th. 3.6] *If X is a finite rack of type D, then X collapses.* $\square$

Therefore, it is very important to determine all simple racks of type D, formally stated as Question 1. The classification of simple racks is known and will be evoked below. We focus on simple racks because of the following reasons:

- If Z is a finite rack and admits a rack epimorphism $\pi : Z \to X$, where X is of type D, then Z is of type D.
- If Z is indecomposable, then it admits a rack epimorphism $\pi : Z \to X$ with X simple.

We collect some criteria on racks of type D, see [**AFGV1**, Subsection 3.2].

- If $Y \subseteq X$ is a subrack of type D, then X is of type D.
- If X is of type D and Z is a rack, then $X \times Z$ is of type D.
- Let K be a subgroup of a finite group G and $\kappa \in C_G(K)$. Let $\mathcal{R}_\kappa : K \to G$ be the map given by $g \mapsto \widetilde{g} := g\kappa$. Let $\mathcal{O}$, resp. $\widetilde{\mathcal{O}}$, be the conjugacy class of $\tau \in K$, resp. of $\widetilde{\tau}$ in G. Then $\mathcal{R}_\kappa$ identifies $\mathcal{O}$ with a subrack of $\widetilde{\mathcal{O}}$. Hence, if $\mathcal{O}$ is of type D, then $\widetilde{\mathcal{O}}$ is of type D.

There is a variation of the last criterium that needs the notion of *quasi-real* conjugacy class. Let G be a finite group, $g \in G$ and $j \in \mathbb{N}$. Recall that $\mathcal{O}_g^G$ is quasi-real of type j if $g^j \neq g$ and $g^j \in \mathcal{O}_g^G$. If g is real, that is $g^{-1} \in \mathcal{O}_g^G$, but not an involution, then $\mathcal{O}_g^G$ is quasi-real of type $\operatorname{ord}(g) - 1$.

Proposition 2.5. [**AFGV1**, Ex. 3.8] *Let G be a finite group and $g = \tau\kappa \in G$, where $\tau \neq e$ and $\kappa \neq e$ commute. Let $K = C_G(\kappa) \ni \tau$; then $\kappa \in C_G(K)$. Hence, the conjugacy class $\mathcal{O}$ of τ in K can be identified with a subrack of the conjugacy class $\widetilde{\mathcal{O}}$ of g in G via $\mathcal{R}_\kappa$ as above. Assume that*

(1) *$\widetilde{\mathcal{O}}$ and $\mathcal{O}$ are quasi-real of type j,*
(2) *the orders N of τ and M of κ are coprime,*
(3) *M does not divide $j - 1$,*
(4) *there exist r_0, $s_0 \in \mathcal{O}$ such that $r_0 \triangleright (s_0 \triangleright (r_0 \triangleright s_0)) \neq s_0$.*

Then $\widetilde{\mathcal{O}}$ is of type D. □

2.5. Simple racks.
Finite simple racks have been classified in [**AG**, Th. 3.9, Th. 3.12]– see also [**J**]. Explicitly, any simple rack falls into one and only one of the following classes:

(1) *Simple affine racks* $(\mathbb{F}_p{}^t, T)$, where p a prime, $t \in \mathbb{N}$, and T is the companion matrix of a monic irreducible polynomial $f \in \mathbb{F}_p[\mathtt{X}]$ of degree t, different from $\mathtt{X}$ and $\mathtt{X} - \mathtt{1}$.

(2) *Non-trivial (twisted) conjugacy classes in simple groups.*

(3) *Simple twisted homogeneous racks*, that is twisted conjugacy classes of type (G, u), where
   - $G = L^t$, with L a simple non-abelian group and $1 < t \in \mathbb{N}$,
   - $u \in \operatorname{Aut}(L^t)$ acts by
   $$u(\ell_1, \dots, \ell_t) = (\theta(\ell_t), \ell_1, \dots, \ell_{t-1}), \quad \ell_1, \dots, \ell_t \in L,$$
   for some $\theta \in \operatorname{Aut}(L)$. Furthermore, L and t are unique, and θ only depends on its conjugacy class in $\operatorname{Out}(L^t)$.

Notation. A *simple rack of type* (L, t, θ) is a twisted homogeneous as in (3).

2.6. The approach by subracks.
The experience shows that the following strategy is useful to approach the study of Nichols algebras over finite groups. However, there are racks that can not be treated in this way.

Strategy. *Let X be a simple rack.*

Step 1: *Is X of type D? In the affirmative, we are done: X and any indecomposable rack Z that admits a rack epimorphism $Z \to X$ collapse, in the sense of Definition 2.2.*

Step 2: *If not, look for the abelian subracks of X. For an abelian subrack S and any $\mathbf{q} \in H^2(X, \mathbb{C}^\times)$, look at the diagonal braiding with matrix $(\mathbf{q}_{ij})_{i,j\in S}$. If the Nichols algebra associated to this diagonal braiding has infinite dimension, and this is known from* [**H2**]*, then so has $\mathfrak{B}(X, \mathbf{q})$. Here you do not need to know all the abelian subracks, just to find one with the above condition.*

Step 3: *Extend the analysis of Step 2 to cocycles of arbitrary degree.*

Step 4: *Extend the analysis of Steps 2 and 3 to indecomposable racks Z that admit a rack epimorphism $Z \to X$.*

The following algorithm is the tool needed to deal with Step 1, when the rack X is realized as a conjugacy class.

Algorithm. *Let Γ be a finite group and let $\mathcal{O}$ be a conjugacy class. Fix $r \in \mathcal{O}$.*

(1) *For any $s \in \mathcal{O}$, check if $(rs)^2 \neq (sr)^2$; this is equivalent to* (10).

(2) *If such s is found, consider the subgroup H generated by r, s. If $\mathcal{O}_r^H \cap \mathcal{O}_s^H = \emptyset$, then $Y = \mathcal{O}_r^H \coprod \mathcal{O}_s^H$ is the decomposable subrack we are looking for and $\mathcal{O}$ is of type D.*

In practice, we implement this algorithm in a recursive way, running over the maximal subgroups, see [**AFGV2**] for details.

Let X be a rack and S a subset of X. We denote $\ll S \gg := \bigcap_{\substack{Y \text{subrack}, \\ S \subset Y \subset X}} Y$. If X is a subrack of a group G and $H = \langle S \rangle$, then $\ll S \gg = \bigcup_{s\in S} \mathcal{O}_s^H$.

There are racks that could not be dealt with the criterium of type D.

Definition 2.6. An indecomposable finite rack X is *of type M* if[2] for any $r, s \in X$, $\ll\{r, s\}\gg$ either is indecomposable or else equals $\{r, s\}$.

There are racks such that all proper subracks are abelian; for instance, the conjugacy class of type $(2, 3)$ in $\mathbb{S}_5$ (here, all proper subracks have at most 2 elements). More examples of racks of type M can be found in [**AFGV1**, Remark 4.2].

3. Tools for cocycles

3.1. The enveloping group.

The enveloping group $\mathbb{G}_X := \langle e_x : x \in X | e_x e_y = e_{x\triangleright y} e_x, x, y \in X\rangle$ was introduced in [**Bk, FR, J**]; it was also considered in [**LYZ, ESS, S**]. The map $e : X \to \mathbb{G}_X$, $x \mapsto e_x$ has a universal property:

If H is a group and $f : X \to H$ is a morphism of racks, then there is a unique morphism of groups $F : \mathbb{G}_X \to H$ such that $F(e_x) = f_x$, $x \in X$.

---

[2]M stands for Montevideo, where this notion was discussed by two of the authors.

In other words, $X \rightsquigarrow \mathbb{G}_X$ is the adjoint of the forgetful functor from groups to racks.

Since $\varphi : X \to \mathbb{S}_X$ is a morphism of racks, there is a group morphism $\Phi : \mathbb{G}_X \to \mathbb{S}_X$. The image, resp. the kernel, of Φ is denoted $\operatorname{Inn}_\triangleright(X)$ (the group of inner automorphisms), resp. Γ_X (the defect group).

The group $\operatorname{Inn}_\triangleright(X)$ is not difficult to compute in the case of our interest. As for the defect group, some properties were established by Soloviev.

Theorem 3.1. (a) *If X is a subrack of a group H, then $\operatorname{Inn}_\triangleright(X) \simeq C/Z(C)$, where C is the subgroup generated by X* [**AG**, Lemma 1.9].

(b) *The defect group Γ_X is central in $\mathbb{G}_X$* [**S**, Th. 2.6]. *Hence $\Gamma_X = Z(\mathbb{G}_X)$ if $\operatorname{Inn}_\triangleright(X)$ is centerless.*

(c) *The rank of Γ_X is the number of $\operatorname{Inn}_\triangleright(X)$-orbits in X* [**S**, Th. 2.10]. $\square$

The difficult part of the calculation of the defect group is to compute its torsion.

Proposition 3.2. *Let $s_i = (i\, i+1) \in \mathbb{S}_m$. Let X be the rack of transpositions in $\mathbb{S}_m$; this is the conjugacy class of s_1. The enveloping group $\mathbb{G}_X$ of X is a central extension*

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{G}_X \longrightarrow \mathbb{S}_m \longrightarrow 0 \tag{11}$$

Proof. By property (a) above, $\operatorname{Inn}_\triangleright(X) \simeq \mathbb{S}_m$. We have to compute Γ_X. Let $\mathbb{B}_m$ be the braid group and as in Subsection 2.2; let $\mathbb{P}_m = \ker \pi$, the pure braid group. We claim that there is a morphism of groups $\Psi : \mathbb{B}_m \to \mathbb{G}_X$ with $\Psi(\sigma_i) = e_{s_i}$, $1 \le i \le m-1$. To prove the claim, we verify the defining relations of the braid group:

$$\text{If } |i-j| \ge 2, \text{ then} \qquad e_{s_i}e_{s_j} = e_{s_i \triangleright s_j}e_{s_i} = e_{s_j}e_{s_i};$$

$$\text{if } |i-j| = 1, \text{ then} \qquad e_{s_i}e_{s_j}e_{s_i} = e_{s_i}e_{s_j \triangleright s_i}e_{s_j} = e_{s_i \triangleright (s_j \triangleright s_i)}e_{s_i}e_{s_j} = e_{s_j}e_{s_i}e_{s_j}$$

since $s_i \triangleright (s_j \triangleright s_i) = s_j$ in $\mathbb{S}_m$. In other words, we have a commutative diagram

$$\begin{tikzcd} \mathbb{B}_m \arrow[rr, "\Psi"] \arrow[dr, "\pi"'] & & \mathbb{G}_X \arrow[dl, "\Phi"] \\ & \mathbb{S}_m. & \end{tikzcd}$$

Clearly, Ψ is surjective and $\ker \Phi = \Psi(\mathbb{P}_m)$. Let now H be a group and $f : X \to H$ a morphism of racks. If $x, y \in X$, then $f_x^2 f_y = f_x f_{x \triangleright y} f_x = f_y f_x^2$ and consequently $f_{y \triangleright x}^2 = f_y f_x^2 f_y^{-1} = f_x^2$. Hence for all $x, y \in X$,

$$f_y^2 = f_x^2 \quad \text{is central in the subgroup generated by } f(X). \tag{12}$$

We call $z = e_{s_i}^2$; this is a central element of $\mathbb{G}_X$ and does not depend on i. Now $\mathbb{P}_m$ is generated by $\tau_{ij} = \sigma_j \triangleright (\sigma_{j+1} \triangleright (\sigma_{j+2} \triangleright \dots \triangleright (\sigma_{i-1} \triangleright \sigma_i^2))$ for all $j < i$, see [**Ar**, page 119],[**Bi**]. Hence $\ker \Phi = \Psi(\mathbb{P}_m)$ is generated by $\Psi(\tau_{ij}) = z$.

Let now V be a vector space with a basis $(v_x)_{x \in X}$ and let $q \in \mathbb{C}$ be a root of 1 of arbitrary order M. Define $f_y \in \mathbf{GL}(V)$ by $f_y(v_x) = q v_{y \triangleright x}$, $x, y \in X$. Then $f_x f_y =$

$f_{x\triangleright y} f_x$ and $f_x^2 = q^2\,\mathrm{id}$ for any $x, y \in X$; thus we have a map $F : \mathbb{G}_X \to \mathbf{GL}(V)$ and $F(z) = q^2\,\mathrm{id}$. This implies that z is not torsion and the claim is proved. □

Remark 3.3. (i). By [**B**, Ch IV, §1, no. 1.9, Prop. 5], there is a section of sets $T : \mathbb{S}_m \to \mathbb{G}_X$ such that $T(ww') = T(w)T(w')$ when $\ell(ww') = \ell(w)\ell(w')$. Thus the central extension corresponds to the cocycle $\eta : \mathbb{S}_m \times \mathbb{S}_m \to \mathbb{Z}$, $\eta(w, w') = T(w)T(w')T(ww')^{-1}$, $w, w' \in \mathbb{S}_m$.

(ii). The proof shows the centrality of Γ_X directly without referring to Theorem 3.1 (b). By Theorem 3.1 (c), z is not torsion; the last paragraph of the proof avoids appealing to this result.

Let $(X, \triangleright)$ be a rack, $\mathbf{q} : X \times X \to \mathbf{GL}(n, \mathbb{C})$ a 2-cocycle of degree n and $(V, c) = (\mathbb{C}X \otimes \mathbb{C}^n, c^{\mathbf{q}})$, *cf.* (7). We discuss how to realize (V, c) as a Yetter-Drinfeld module over a group algebra. Let $x \in X$ and define $g_x : V \to V$ by

$$g_x(e_y w) = e_{x\triangleright y} \mathbf{q}_{x,y}(w), \qquad y \in X, w \in \mathbb{C}^n, \tag{13}$$

and let $\mathrm{Inn}_{X,\mathbf{q}}$ be the subgroup of $\mathbf{GL}(V)$ generated by the g_x's, $x \in X$. Then $g_x g_y = g_{x\triangleright y} g_x$ for any $x, y \in X$, and (V, c) is a Yetter-Drinfeld module over the group algebra of $\mathrm{Inn}_{X,\mathbf{q}}$, with the natural action and coaction $\delta(e_x v) = g_x \otimes e_x v$, $x \in X$, $v \in \mathbb{C}^n$.

Lemma 3.4. *Let F be a group provided with:*

- *a group homomorphism $p : F \to \mathrm{Inn}_{X,\mathbf{q}}$;*
- *a rack homomorphism $s : X \to F$ such that $p(s_x) = g_x$ and F is generated as a group by $s(X)$.*

Then $(V, c) \in {}^{\mathbb{C}F}_{\mathbb{C}F}\mathcal{YD}$, with the action induced by p and coaction $\delta(e_x v) = s_x \otimes e_x v$, $x \in X$, $v \in \mathbb{C}^n$. In particular, $(V, c) \in {}^{\mathbb{C}\mathbb{G}_X}_{\mathbb{C}\mathbb{G}_X}\mathcal{YD}$.

Proof. If $x, y \in X$ and $w \in \mathbb{C}^n$, then $\delta(s_x \cdot e_y w) = \delta(e_{x\triangleright y}\mathbf{q}_{x,y}(w)) = s_{x\triangleright y} \otimes e_{x\triangleright y}\mathbf{q}_{x,y}(w) = s_x s_y s_x^{-1} \otimes e_{x\triangleright y}\mathbf{q}_{x,y}(w) = s_x s_y s_x^{-1} \otimes s_x \cdot w$. Since F is generated by $s(X)$, it follows that $\delta(f \cdot e_y w) = f s_y f^{-1} \otimes f \cdot w$, for all $f \in F$. □

As a consequence, the Nichols algebra of the braided vector space $(\mathbb{C}X, c_q)$ bears a $\mathbb{G}_X$-grading, that we shall call the *principal* grading, as opposed to the natural $\mathbb{N}$-grading. Indeed, if X is abelian, then $\mathbb{G}_X \simeq \mathbb{Z}^{\mathrm{card}\, X}$ and the principal grading coincides with the one considered *e. g.* in [**AHS**].

3.2. The rack cohomology group $H^2(X, \mathbb{C}^\times)$.

We now state some general facts about the cocycles on a rack X with values in the abelian group $\mathbb{C}^\times$. In this case, the H^2 is part of a cohomology theory, see [**AG**] and references therein. An alternative description of $H^2(X, \mathbb{C}^\times)$ was found in [**EGñ**] through the enveloping group. Namely, let $\mathrm{Fun}(X, \mathbb{C}^\times)$ be the space of all functions from X to $\mathbb{C}^\times$ with right $\mathbb{G}_X$-action given by $(f \cdot e_x)(y) = f(x \triangleright y)$, $f : X \to A$, $x, y \in X$.

Lemma 3.5. [**EGñ**] $H^2(X, \mathbb{C}^\times) \simeq H^1(\mathbb{G}_X, \mathrm{Fun}(X, \mathbb{C}^\times))$. □

In principle, the cohomology of $\mathbb{G}_X$ could be studied via the Hochschild-Serre sequence from that of $\mathrm{Inn}_\triangleright(X)$ and Γ_X. However, the computation of the defect group seems to be very difficult. There is also a homology theory of racks, related to the computation we are interested in by the following result.

Lemma 3.6. [**AG**, Lemma 4.7] $H^2(X,\mathbb{C}^\times) \simeq \mathit{Hom}(H_2(X,\mathbb{Z}),\mathbb{C}^\times)$. $\square$

There is a monomorphism $\mathbb{C}^\times \hookrightarrow H^2(X,\mathbb{C}^\times)$, since any constant function is a cocycle. A natural question is to compute the quotient $H^2(X,\mathbb{C}^\times)/\mathbb{C}^\times$. *Assume that X is indecomposable.* If $\mathbf{q} \in Z^2(X,\mathbb{C}^\times)$, then

$$\mathbf{q}_{ii} = \mathbf{q}_{jj}, \quad \text{for any } i,j \in X. \tag{14}$$

Note also that $\mathbf{q} \sim \widetilde{\mathbf{q}}$ as in (8) implies that $\mathbf{q}_{ii} = \widetilde{\mathbf{q}}_{ii}$ for all $i \in X$. Therefore the question can be rephrased as follows.

Question 4. *Compute all cocycles $\mathbf{q} \in Z^2(X,\mathbb{C}^\times)$ such that $\mathbf{q}_{ii} = -1$.*

3.3. The program RiG.

A program for calculations with racks, that in particular computes the rack-(co)homology groups, was developed in [**GV**]. We use it to compute some cohomology groups of simple racks that are not of type D, see Theorems 5.1 and 6.1.

Proposition 3.7. *Let $\sigma \in \mathbb{S}_m$ be of type $(1^{n_1}, 2^{n_2}, \dots, m^{n_m})$ and let*

$$\mathcal{O} = \begin{cases} (a) & \textit{the conjugacy class of } \sigma \textit{ in } \mathbb{S}_m, \quad \textit{if } \sigma \notin \mathbb{A}_m, \\ (b) & \textit{the conjugacy class of } \sigma \textit{ in } \mathbb{A}_m, \quad \textit{if } \sigma \in \mathbb{A}_m. \end{cases}$$

(a) *If $m = 5$ and the type is $(2,3)$, then $H^2(\mathcal{O},\mathbb{C}^\times) = \mathbb{C}^\times \times \mathbb{G}_6$.*
(b) *If $m = 6,7,8$ and the type is $(1^n,2)$, then $H^2(\mathcal{O},\mathbb{C}^\times) = \mathbb{C}^\times \times \mathbb{G}_2$.*
(c) *If $m = 6$ and the type is (2^3), then $H^2(\mathcal{O},\mathbb{C}^\times) = \mathbb{C}^\times \times \mathbb{G}_2$.*
(d) *If $m = 5$ and the type is $(1^2,3)$, then $H^2(\mathcal{O},\mathbb{C}^\times) = \mathbb{C}^\times \times \mathbb{G}_6$.*
(e) *If $m = 6$ and the type is $(1,2,3)$, then $H^2(\mathcal{O},\mathbb{C}^\times) = \mathbb{C}^\times \times \mathbb{G}_3 \times \mathbb{G}_6$.*

TABLE 1. Some homology groups of conjugacy classes in $\mathbb{S}_m$.

type of X		$H_2(X,\mathbb{Z})$
$\mathbb{S}_5$	$(1\,2)(3\,4\,5)$	$\mathbb{Z} \oplus \mathbb{Z}/6$
$\mathbb{A}_5$	$(1\,2\,3)$	$\mathbb{Z} \oplus \mathbb{Z}/6$
$\mathbb{S}_6$	$(1\,2)(3\,4)(5\,6)$	$\mathbb{Z} \oplus \mathbb{Z}/2$
$\mathbb{S}_6$	$(1\,2)$	$\mathbb{Z} \oplus \mathbb{Z}/2$
$\mathbb{A}_6$	$(1\,2\,3)$	$\mathbb{Z} \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/6$
$\mathbb{S}_7$	$(1\,2)$	$\mathbb{Z} \oplus \mathbb{Z}/2$
$\mathbb{S}_8$	$(1\,2)$	$\mathbb{Z} \oplus \mathbb{Z}/2$

PROOF. We use GAP and RiG to compute the homology groups $H_2(\mathcal{O},\mathbb{Z})$. These results are listed in Table 1. Now assume X is a rack and that there exists $m \in \mathbb{N}_{\geq 2}$ such that $H_2(X,\mathbb{Z}) \simeq \mathbb{Z} \oplus \mathbb{Z}/m_1 \oplus \cdots \oplus \mathbb{Z}/m_r$. By Lemma 3.6, we have

$H^2(X,\mathbb{C}^\times) \simeq \operatorname{Hom}(\mathbb{Z}\oplus\mathbb{Z}/m_1\oplus\cdots\oplus\mathbb{Z}/m_r,\mathbb{C}^\times) \simeq \operatorname{Hom}(\mathbb{Z},\mathbb{C}^\times)\times\operatorname{Hom}(\mathbb{Z}/m_1,\mathbb{C}^\times)\times\cdots\times\operatorname{Hom}(\mathbb{Z}/m_r,\mathbb{C}^\times)\simeq\mathbb{C}^\times\times\mathbb{G}_{m_1}\times\cdots\times\mathbb{G}_{m_r}$. □

3.4. Twisting.

There is a method, called twisting, to deform the the multiplication of a Hopf algebra [**DT**]; it is formally dual to the twisting of the comultiplication [**D, R**]. The relation with bosonization was established in [**MO**]. Here we show how to relate two cocycles over a rack X by a twisting, in a way that the corresponding Nichols algebras are preserved.

Let $\mathcal{H}$ be a Hopf algebra. Let $\phi:\mathcal{H}\otimes\mathcal{H}\to\mathbb{C}$ be an invertible (with respect to the convolution) linear map and define a new product by $x\cdot_\phi y = \phi(x_{(1)},y_{(1)})x_{(2)}y_{(2)}\phi^{-1}(x_{(3)},y_{(3)})$, $x,y\in\mathcal{H}$. If ϕ is a unitary 2-cocycle, that is for all $x,y,z\in\mathcal{H}$,

$$\phi(x_{(1)}\otimes y_{(1)})\,\phi(x_{(2)}y_{(2)}\otimes z)=\phi(y_{(1)}\otimes z_{(1)})\,\phi(x\otimes y_{(2)}z_{(2)}), \tag{15}$$

$$\phi(x\otimes 1)=\phi(1\otimes x)=\varepsilon(x), \tag{16}$$

then $\mathcal{H}_\phi$ (the same coalgebra but with multiplication $\cdot_\phi$) is a Hopf algebra.

Theorem 3.8. [**MO**, 2.7, 3.4] *Let $\phi:\mathcal{H}\otimes\mathcal{H}\to\mathbb{C}$ be an invertible unitary 2-cocycle.*

(a) *There exists an equivalence of braided categories $\mathcal{T}_\phi: {}^{\mathcal{H}}_{\mathcal{H}}\mathcal{YD}\to{}^{\mathcal{H}_\phi}_{\mathcal{H}_\phi}\mathcal{YD}$, $V\mapsto V_\phi$, which is the identity on the underlying vector spaces, morphisms and coactions, and transforms the action of $\mathcal{H}$ on V to $\cdot_\phi:\mathcal{H}_\phi\otimes V_\phi\to V_\phi$,*

$$h\cdot_\phi v=\phi(h_{(1)},v_{(-1)})(h_{(2)}\cdot v_{(0)})_{(0)}\,\phi^{-1}((h_{(2)}\cdot v_{(0)})_{(-1)},h_{(3)}),$$

$h\in\mathcal{H}_\phi$, $v\in V_\phi$. The monoidal structure on $\mathcal{T}_\phi$ is given by the natural transformation $b_{V,W}:(V\otimes W)_\phi\to V_\phi\otimes W_\phi$

$$b_{V,W}(v\otimes w)=\phi(v_{(-1)},w_{(-1)})v_{(0)}\otimes w_{(0)},\quad v\in V, w\in W.$$

(b) *$\mathcal{T}_\phi$ preserves Nichols algebras: $\mathfrak{B}(V)_\phi\simeq\mathfrak{B}(V_\phi)$ as objects in ${}^{\mathcal{H}_\phi}_{\mathcal{H}_\phi}\mathcal{YD}$. In particular, the Poincaré series of $\mathfrak{B}(V)$ and $\mathfrak{B}(V_\phi)$ are the same.* □

Let us recall the argument for (ii). The functor $\mathcal{T}_\phi$ preserves the braidings; that is, if c, resp. c_ϕ, is the braiding in ${}^{\mathcal{H}}_{\mathcal{H}}\mathcal{YD}$, resp. ${}^{\mathcal{H}_\phi}_{\mathcal{H}_\phi}\mathcal{YD}$, then the following diagram commutes:

$$\begin{tikzcd} (V\otimes W)_\phi \arrow[r, "\mathcal{T}_\phi(c)"] \arrow[d, "b_{V,W}"'] & (W\otimes V)_\phi \arrow[d, "b_{W,V}"] \\ V_\phi\otimes W_\phi \arrow[r, "c_\phi"] & W_\phi\otimes V_\phi. \end{tikzcd} \tag{17}$$

Since the ideal of relations of a Nichols algebra is the sum of the kernels of the various quantum symmetrizers, (ii) follows immediately.

Let G be a group. If $\mathcal{H}=\mathbb{C}G$, then a unitary 2-cocycle on $\mathcal{H}$ is equivalent to a 2-cocycle $\phi\in Z^2(G,\mathbb{C}^\times)$, that is a map $\phi:G\times G\to\mathbb{C}^\times$ such that

$$\phi(g,h)\,\phi(gh,t)=\phi(h,t)\,\phi(g,ht) \tag{18}$$

and $\phi(g,e)=\phi(e,g)=1$ for all $g,h,t\in G$.

Let $\sigma, \zeta \in G$, $\mathcal{O}_\sigma$, $\mathcal{O}_\zeta$ their conjugacy classes, $(\rho, V) \in \widehat{C_G(\sigma)}$, $(\tau, W) \in \widehat{C_G(\zeta)}$. For $\nu \in \mathcal{O}_\sigma$, $\xi \in \mathcal{O}_\zeta$, pick $g_\nu, h_\xi \in G$ such that $g_\nu \triangleright \sigma = \nu$, $h_\xi \triangleright \zeta = \xi$.

Lemma 3.9. *If $\phi \in Z^2(G, \mathbb{C}^\times)$, then the braiding*

$$c_\phi : M(\mathcal{O}_\sigma, \rho)_\phi \otimes M(\mathcal{O}_\zeta, \tau)_\phi \to M(\mathcal{O}_\zeta, \tau)_\phi \otimes M(\mathcal{O}_\sigma, \rho)_\phi$$

is given by

$$c_\phi(g_\nu v \otimes h_\xi w) = \phi(\nu, \xi)\phi^{-1}(\nu \triangleright \xi, \nu)\, \nu \cdot h_\xi w \otimes g_\nu v, \tag{19}$$

$v \in V$, $w \in W$.

Proof. By (17), since $b_{M(\mathcal{O}_\sigma,\rho),M(\mathcal{O}_\zeta,\tau)}(g_\nu v \otimes h_\xi w) = \phi(\nu, \xi)\, g_\nu v \otimes h_\xi w$. $\square$

Let now X be a subrack of a conjugacy class $\mathcal{O}$ in G, q a 2-cocycle on X arising from some Yetter-Drinfeld module $M(\mathcal{O}, \rho)$ with $\dim \rho = 1$ and $\phi \in Z^2(G, \mathbb{C}^\times)$. Define $q^\phi : X \times X \to \mathbb{C}^\times$ by

$$q^\phi_{xy} = \phi(x, y)\phi^{-1}(x \triangleright y, x)\, q_{xy}, \quad x, y \in X. \tag{20}$$

Then Lemma 3.9 and Th. 3.8 imply that

(21) The Poincaré series of $\mathfrak{B}(X, q)$ and $\mathfrak{B}(X, q^\phi)$ are equal.

Remark 3.10. If X is any rack, q a 2-cocycle on X and $\phi : X \times X \to \mathbb{C}^\times$, then define q^ϕ by (20). It can be shown that q^ϕ is a 2-cocycle iff

$$\begin{aligned}\phi(x, z)\phi(x \triangleright y, x \triangleright z)\phi(x \triangleright (y \triangleright z), x)\phi(y \triangleright z, y)& \\ = \phi(y, z)\phi(x, y \triangleright z)\phi(x \triangleright (y \triangleright z), x \triangleright y)\phi(x \triangleright z, x)&\end{aligned} \tag{22}$$

for any $x, y, z \in X$. Thus, if X is a subrack of a group G and $\phi \in Z^2(G, \mathbb{C}^\times)$, then $\phi|_{X\times X}$ satisfies (22).

Definition 3.11. The 2-cocycles q and q' on X are *equivalent by twist* if there exists $\phi : X \times X \to \mathbb{C}^\times$ such that $q' = q^\phi$ as in (20).

4. Simple affine racks

Let p be a prime, $t \in \mathbb{N}$ and $f \in \mathbb{F}_p[\mathtt{X}]$ of degree t, monic irreducible and different from $\mathtt{X}$ and $\mathtt{X} - \mathtt{1}$. Let T be the companion matrix of f and $\mathsf{Q}_{\mathbb{F}_p^t, f} := \mathsf{Q}_{\mathbb{F}_p^t, T}$ be the associated affine rack; this will be simply denoted by Q if no emphasis is needed. Alternatively, set $q = p^t$ and identify $\mathbb{F}_q$ with $\mathbb{F}_p^t$. Then the action of T corresponds to multiplication by a, which is the class of $\mathtt{X}$ in $\mathbb{F}_p[\mathtt{X}]/(\mathtt{f})$. Note that a generates $\mathbb{F}_q$ over $\mathbb{F}_p$.

Question 5. *Find the proper subracks of Q.*

We expect that the simple affine racks will have very few subracks. In fact, they have no abelian subracks with more than one element [**AFGV1**, Remark 3.13].

Proposition 4.1. *If a generates $\mathbb{F}_q^\times$, then any proper subrack of $\mathsf{Q}_{\mathbb{F}_q, a}$ is trivial.*

Proof. Let X be a subrack of $\mathsf{Q}_{\mathbb{F}_q,a}$ with more than one element. Let $x, y \in X$ with $x \neq y$. By definition we have $\varphi_x^n(y) \in X$ for all $n \in \mathbb{N}$. Since $\varphi_x^n(y) = (1-a^n)x + a^n y$, for all $n \in \mathbb{N}$, we have that

$$A = \{(1-a^n)x + a^n y \mid 0 \leq n \leq q-1\} \subseteq X.$$

Moreover, A has q elements. Indeed, suppose there exist $m \neq n$ such that $(1-a^n)x + a^n y = (1-a^m)x + a^m y$. Then $x(a^m - a^n) = y(a^m - a^n)$ which implies that $x = y$, a contradiction. Since $A \subseteq X \subseteq \mathsf{Q}_{\mathbb{F}_q,a}$ and $|\mathsf{Q}_{\mathbb{F}_q,a}| = q$ we have that $X = \mathsf{Q}_{\mathbb{F}_q,a}$. □

In the particular case $t = 1$, we can say more: any proper subrack of an affine rack with p elements is trivial.

Proposition 4.2. *Let $1 \neq a \in \mathbb{F}_p^\times$. Then any proper subrack of the affine rack $\mathsf{Q}_{\mathbb{F}_p,a}$ is trivial.*

Proof. Let $x \neq y$ be two elements of $\mathbb{F}_p$. It is enough to show that the subrack generated by x and y is $\mathbb{F}_p$. Let

$$F_{a,m}(n_1, n_2, ..., n_m) = \sum_{j=1}^{m} (-1)^{j+1} a^{n_j + \dots + n_m}.$$

Note that $a + aF_{a,2k}(n_1, n_2, ..., n_{2k}) = F_{a,2k+1}(n_1, n_2, ..., n_{2k}, 1)$. Then

$$\varphi_y^{n_{2k}} \varphi_x^{n_{2k-1}} \cdots \varphi_x^{n_1}(y) = y + (y-x)F_{a,2k}(n_1, n_2, ..., n_{2k}), \tag{23}$$

$$\varphi_y^{n_{2k+1}} \varphi_x^{n_{2k}} \cdots \varphi_x^{n_1}(y) = x + (y-x)F_{a,2k+1}(n_1, n_2, ..., n_{2k+1}). \tag{24}$$

Let $z \in \mathbb{F}_p$, then

$$z = \varphi_y^{n_{2k}} \varphi_x^{n_{2k-1}} \cdots \varphi_x^{n_1}(y) \tag{25}$$

has at least one solution. In fact, let $n_j = (-1)^j$. Equation (23) implies that (25) can be re-written as $z = y + (y-x)(1-a)k$. Then the result follows by taking $k = (z-y)(1-a)^{-1}(y-x)^{-1}$. □

5. Conjugacy classes in non-abelian simple groups

5.1. Alternating groups.

Let $\sigma \in \mathbb{S}_m$. We say that σ is of type $(1^{n_1}, 2^{n_2}, \dots, m^{n_m})$ if the decomposition of σ as product of disjoint cycles contains n_j cycles of length j, for every j, $1 \leq j \leq m$.

Theorem 5.1. [**AFGV1**, Th. 4.1] *Let $\sigma \in \mathbb{A}_m$, $m \geq 5$. If the type of σ is NOT any of (3^2); $(2^2, 3)$; $(1^n, 3)$; (2^4); $(1^2, 2^2)$; $(1, 2^2)$; $(1, p)$, (p) with p prime, then the conjugacy class of σ in $\mathbb{A}_m$ is of type D.* □

5.2. Sporadic groups.

Theorem 5.2. [**AFGV2, AFGV3**] *If G is a sporadic simple group and $\mathcal{O}$ is a non-trivial conjugacy class of G NOT listed in Table 2, then $\mathcal{O}$ is of type D.* □

Table 2. Conjugacy classes of sporadic groups not known of type D; those which are NOT of type D appear in bold.

G	**Classes**	G	**Classes**
M_{11}	**8A, 8B, 11A, 11B**	Co_1	3A, 23A, 23B
M_{12}	**11A, 11B**	J_1	**15A, 15B, 19A, 19B, 19C**
M_{22}	**11A, 11B**	$O'N$	31A, 31B
M_{23}	**23A, 23B**	J_3	5A, 5B, 19A, 19B
M_{24}	**23A, 23B**	Ru	29A, 29B
J_2	**2A, 3A**	He	all of type D
Suz	3A	Fi_{22}	**2A**, 22A, 22B
HS	11A, 11B	Fi_{23}	**2A**, 23A, 23B
McL	11A, 11B	HN	all of type D
Co_3	23A, 23B	Th	all of type D
Co_2	**2A**, 23A, 23B	T	2A

G	**Classes**
Ly	33A, 33B, 37A, 37B, 67A, 67B, 67C
J_4	29A, 37A, 37B, 37C, 43A, 43B, 43C
Fi'_{24}	23A, 23B, 27B, 27C, 29A, 29B, 33A, 33B, 39C, 39D
B	2A, 16C, 16D, 32A, 32B, 32C, 32D, 34A,
	46A, 46B, 47A, 47B
M	32A, 32B, 41A, 46A, 46B, 47A, 47B, 59A, 59B,
	69A, 69B, 71A, 71B, 87A, 87B, 92A, 92B, 94A, 94B

5.3. Finite groups of Lie type.

Let p be a prime number, $m \in \mathbb{N}$ and $q = p^m$. Let $\mathbb{G}$ be an algebraic reductive group defined over the algebraic closure of $\mathbb{F}_q$ and $G = \mathbb{G}(\mathbb{F}_q)$ be the finite group of $\mathbb{F}_q$-points. Let $x \in G$; we want to investigate the orbit $\mathcal{O}_x^G$ of x in G. Let $x = x_s x_u$ be the Chevalley-Jordan decomposition of x in $\mathbb{G}$; then $x_s, x_u \in G$. Let $\mathbb{K} = C_{\mathbb{G}}(x_s)$, a reductive subgroup of $\mathbb{G}$ by [**Hu**, Thm. 2.2], and let $\mathbb{L}$ be its semisimple part; then $K := \mathbb{K} \cap G = C_G(x_s)$, by [**Bo**, Prop. 9.1]. Since $x_u \in K$, we conclude from Subsection 2.4 that

$$\mathcal{O}_{x_u}^K \text{ is a subrack of } \mathcal{O}_x^G.$$

Therefore, we are reduced to investigate the orbits $\mathcal{O}_x$ when x is either semisimple (the case $x = x_s$) or unipotent (by the reduction described).

The first step of the Strategy proposed in Subsection 2.6 consists of finding subracks of type D of conjugacy classes of semisimple or unipotent elements. We believe that most semisimple conjugacy classes are of type D. We give now some evidence for this belief, using techniques with involutions and elements of a Weyl group associated to a fixed $\mathbb{F}_q$-split torus.

Let $n > 1$, $\xi \in \mathbb{F}_q^\times$ so that $\operatorname{ord}\xi = m$ divides $q-1$ and $a \in \mathbb{F}_q^\times$. For all $x = (x_1, \dots, x_n) \in (\mathbb{Z}/m)^n$ such that $\sum_{i=0}^n x_i \equiv 0 \pmod m$ define n_a to be the companion matrix of the polynomial $X^n - a$, $\xi_x = \operatorname{diag}(\xi^{x_1}, \dots, \xi^{x_n})$ and $\mu_x = n_a \xi_x$.

$$\mu_x = \begin{pmatrix} 0 & & \dots & 0 & a\xi^{x_n} \\ \xi^{x_1} & 0 & \dots & 0 & 0 \\ 0 & \xi^{x_2} & \dots & 0 & \vdots \\ \vdots & & \ddots & \vdots & 0 \\ 0 & \dots & \dots & \xi^{x_{n-1}} & 0 \end{pmatrix} \in \mathbf{GL}(n, \mathbb{F}_q).$$

Let $X_{a,\xi} = \{\mu_x : \sum_{i=1}^n x_i \equiv 0 \pmod m\}$, a subset of the conjugacy class of n_a in $\mathbf{GL}(n, \mathbb{F}_q)$ (that is, the set of matrices with minimal polynomial $T^n - a$). If $a = -1$, then $X_{a,\xi} \subseteq \mathbf{SL}(n, \mathbb{F}_q)$.

The following proposition is a generalization of [**AF3**, Example 3.15].

Proposition 5.3. *Assume that $(n, q-1) \neq 1$; that $q > 3$, if $n = 4$; and that $q > 5$, if $n = 2$. Then the conjugacy class of n_a is of type D.*

Proof. Pick a generator ξ of $\mathbb{F}_q^\times$. We claim that $X_{a,\xi}$ is a subrack of the conjugacy class of n_a in $\mathbf{GL}(n, \mathbb{F}_q)$, isomorphic to the affine rack $\mathsf{Q}_{(\mathbb{Z}/(q-1))^{n-1}, g}$, with $g(x_1, \dots, x_{n-1}) = \left(-\sum_{i=1}^{n-1} x_i, x_1, \dots, x_{n-2}\right)$. A direct computation shows that $\mu_x \mu_y \mu_x^{-1} = \mu_{x \triangleright y}$, with

$$x \triangleright y = (x_1 + y_n - x_n, x_2 + y_1 - x_1, \dots, x_n + y_{n-1} - x_{n-1}).$$

Thus, the map $\varphi : X_{a,\xi} \to \mathsf{Q}_{(\mathbb{Z}/(q-1))^{n-1}, g}$ given by $\varphi(\mu_x) = (x_1, \dots, x_{n-1})$ is a rack isomorphism and the claim is proved. The proposition follows now from [**AFGaV**, Lemma 2.2], for $n > 2$, or [**AFGaV**, Lemma 2.1], for $n = 2$. $\square$

The conjugacy class of involutions in $\mathbf{PSL}(2, \mathbb{F}_q)$ for $q \in \{5, 7, 9\}$ is not of type D. For $q > 9$ we have the following result.

Corollary 5.4. (a) *Assume that $q \equiv 1 \pmod 4$ and $q > 9$. Then the conjugacy class of involutions of $\mathbf{PSL}(2, \mathbb{F}_q)$ is of type D.*

(b) *Assume that $q \equiv 3 \pmod 4$ and $q > 9$. Then the conjugacy class of involutions of $\mathbf{PGL}(2, \mathbb{F}_q)$ is of type D.*

Proof. (a) Let $\xi \in \mathbb{F}_q$ such that $\mathbb{F}_q^\times = \langle \xi \rangle$. By Proposition 5.3 with $a = -1$, the subrack $X = \{\left(\begin{smallmatrix} 0 & -\xi^{-x} \\ \xi^x & 0 \end{smallmatrix}\right) : x \in \mathbb{Z}/(q-1)\}$ of the conjugacy class of n_{-1} in $\mathbf{GL}(2, \mathbb{F}_q)$ is isomorphic to the dihedral rack $\mathcal{D}_{q-1}$. Let $\pi : \mathbf{GL}(2, \mathbb{F}_q) \to \mathbf{PGL}(2, \mathbb{F}_q)$ be the canonical projection. Then $\pi\left(\begin{smallmatrix} 0 & -\xi^{-x} \\ \xi^x & 0 \end{smallmatrix}\right) \in \mathbf{PSL}(2, \mathbb{F}_q)$ for all $x \in \mathbb{Z}/(q-1)$ and whence $\pi(X)$ is a subrack of the unique conjugacy class of involutions in $\mathbf{PSL}(2, \mathbb{F}_q)$. Now $\pi\left(\begin{smallmatrix} 0 & -\xi^{-x} \\ \xi^x & 0 \end{smallmatrix}\right) = \pi\left(\begin{smallmatrix} 0 & -\xi^{-y} \\ \xi^y & 0 \end{smallmatrix}\right)$ iff $\xi^x = -\xi^y$, hence $\pi(X) \simeq \mathcal{D}_{(q-1)/2}$, which is of type D if $(q-1)/2$ is even and > 4.

(b) Let $L = \{\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) : a, b \in \mathbb{F}_q\}$. Then L is a quadratic field extension of $\mathbb{F}_q$ and $|L| = q^2$. Consider now the group map $\det : L^\times \to \mathbb{F}_q^\times$ given by the determinant. Since every element in a finite field is a sum of squares, the kernel is a subgroup of $L^\times$ of order $\frac{|L^\times|}{|\mathbb{F}_q^\times|} = \frac{q^2-1}{q-1}$. Since $L^\times$ is cyclic, there exist $a, b \in \mathbb{F}_q$

such that $a^2+b^2=1$ and $\theta = \left(\begin{smallmatrix} a & b \\ -b & a\end{smallmatrix}\right)$ generates $\ker\det$, *i.e.* it has order $q+1$. Note that, as $q \equiv 3 \pmod 4$, θ is contained in a non-split torus.

Let $n = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0\end{smallmatrix}\right)$. Then the subrack $X = \{\mu_x = n\theta^x : x \in \mathbb{Z}/(q+1)\}$ of the conjugacy class of n in $\mathbf{GL}(2,\mathbb{F}_q)$ is isomorphic to the dihedral rack $\mathcal{D}_{q+1}$. Taking π as in (a), we have that $\pi(X) \simeq \mathcal{D}_{(q+1)/2}$ is a subrack of the unique conjugacy class of involutions in $\mathbf{PGL}(2,\mathbb{F}_q)$, which is of type D if $(q+1)/2$ is even and >4. $\square$

A similar argument as in the proof of proposition 5.3 applies with weaker hypothesis to matrices whose rational form contains n_a.

Proposition 5.5. *Let $x \in \mathbf{GL}(N,\mathbb{F}_q)$ be a semisimple element whose rational form x is $\left(\begin{smallmatrix} n_a & 0 \\ 0 & B_1\end{smallmatrix}\right)$. Suppose there exists $B_2 \in \mathbf{GL}(N-n,\mathbb{F}_q)$ such that $B_2 \neq B_1$, $B_2 \sim B_1$ and $B_1B_2 = B_2B_1$. Then the conjugacy class of x is of type D for all $n \neq 2,4$; or $n=4$ and $q>3$; or $n=2$ and q is odd.*

Proof. Pick a generator ξ of $\mathbb{F}_q^\times$ and let μ_x be as above. Let

$$X_i = \left\{\left(\begin{smallmatrix} \mu_x & 0 \\ 0 & B_i\end{smallmatrix}\right) : \sum_{j=1}^n x_j \equiv 0 \pmod{q} - 1\right\},$$

$i=1,2$ and $X = X_1 \coprod X_2$. Since $\left(\begin{smallmatrix} \mu_x & 0 \\ 0 & B_i\end{smallmatrix}\right) \triangleright \begin{pmatrix} \mu_y & 0 \\ 0 & B_j\end{pmatrix} = \begin{pmatrix} \mu_{x\triangleright y} & 0 \\ 0 & B_j\end{pmatrix}$ and $X_1 \cap X_2 = \emptyset$, we see that X is a decomposable rack and each X_i is isomorphic to an affine rack, by the proof of Proposition 5.3. If $x=(0,\dots,0)$, $y=(1,0,\dots,0)$, $s = \left(\begin{smallmatrix} \mu_x & 0 \\ 0 & B_1\end{smallmatrix}\right)$ and $r = \begin{pmatrix} \mu_y & 0 \\ 0 & B_2\end{pmatrix}$, then $r \triangleright (s \triangleright (r \triangleright s)) \neq s$, by a straightforward computation, see the proof of [**AFGaV**, Lemma 2.2], whenever the prescribed restrictions on n hold. $\square$

Assume now that $\mathbb{G}$ be a Chevalley group and denote by $G = \mathbb{G}(\mathbb{F}_q)$ the group of $\mathbb{F}_q$-points. Let T be a $\mathbb{F}_q$-split torus in G and $W = N_G(T)/C_G(T)$ the corresponding Weyl group. Let $\sigma \in W$ and $n_\sigma \in N_G(T)$ be a representant of σ. Since W stabilizes T, the adjoint action of n_σ on T defines an automorphism g_σ of $(\mathbb{Z}/(q-1))^n$. Indeed, without loss of generality, we may assume that $T = \mathbb{F}_q^\times \times \cdots \times \mathbb{F}_q^\times$ and $\mathbb{F}_q^\times = \langle\xi\rangle$, with $\xi \in \mathbb{F}_q^\times$. Then for all $t \in T$, there exists $x \in (\mathbb{Z}/(q-1))^n$ such that $t = \xi_x = \operatorname{diag}(\xi^{x_1},\dots,\xi^{x_n})$, $n = \dim T$, and the automorphism is defined by $n_\sigma \xi_x n_\sigma^{-1} = \xi_{g_\sigma(x)}$.

The following proposition is a generalization of Proposition 5.3.

Proposition 5.6. *Let $\sigma \in W$ and $n_\sigma \in N_G(T)$ be a representant of σ. Assume there exists $x \in (\mathbb{Z}/(q-1))^n$ such that $x \notin \operatorname{Im}(\mathrm{id} - g_\sigma)$ and $x - g_\sigma(x) + g_\sigma^2(x) - g_\sigma^3(x) \neq 0$. Then the conjugacy class of n_σ in G is of type D.*

Proof. Consider the set $X_{\sigma,\xi} = \{\mu_y = n_\sigma \xi_y : y \in (\mathbb{Z}/(q-1))^n\}$. Then $X_{\sigma,\xi}$ is a (non-empty) rack isomorphic to the affine rack $((\mathbb{Z}/(q-1))^n, g_\sigma)$. Indeed, since

$$\begin{aligned}\mu_x\mu_y\mu_x^{-1} &= n_\sigma\xi_x n_\sigma \xi_y \xi_x^{-1} n_\sigma^{-1} = n_\sigma \xi_x n_\sigma \xi_{y-x} n_\sigma^{-1} = n_\sigma \xi_x \xi_{g_\sigma(y-x)} \\ &= n_\sigma \xi_{g_\sigma(y) + (1-g_\sigma)(x)} = \mu_{x\triangleright y},\end{aligned}$$

the map $\varphi : X_{\sigma,\xi} \to ((\mathbb{Z}/(q-1))^n, g_\sigma)$ given by $\varphi(\mu_x) = x$ defines a rack isomorphism. Since $x \notin \operatorname{Im}(\operatorname{id} - g_\sigma)$, $X_{\sigma,\xi}$ contains at least two cosets with respect to $\operatorname{Im}(1 - g_\sigma)$. If we take $s = \mu_0$ and $r = \mu_x$, then

$$r \triangleright (s \triangleright (r \triangleright s)) = \mu_{x \triangleright (0 \triangleright (x \triangleright 0))} = \mu_{x - g_\sigma(x) + g_\sigma^2(x) - g_\sigma^3(x)},$$

which implies that $X_{\sigma,\xi}$ is of type D. □

6. Twisted conjugacy classes in simple non-abelian groups

In this section we consider twisted conjugacy classes in simple non-abelian groups defined by non-trivial outer automorphisms. These can be realized as conjugacy classes in the following way. Pick a representant of θ in $\operatorname{Aut}(L)$, called also θ, and form the semidirect product $L \rtimes \langle\theta\rangle$. Then the racks of type $(L, 1, \theta)$ are the conjugacy classes of $L \rtimes \langle\theta\rangle$ contained in $L \times \{\theta\}$.

6.1. Alternating groups.

Since $\mathbb{A}_m \rtimes \mathbb{Z}/2 \simeq \mathbb{S}_m$, the racks of this type are the conjugacy classes in $\mathbb{S}_n$ do not intersecting $\mathbb{A}_n$. We keep the notation from subsection 5.1. Assume that $m \geq 5$.

Theorem 6.1. [**AFGV1**, Th. 4.1] *Let $\sigma \in \mathbb{S}_m - \mathbb{A}_m$. If the type of σ is neither $(2,3)$, nor (2^3), nor $(1^n, 2)$, then the conjugacy class of σ is of type D.* □

Notice that the racks of type (2^3) and $(1^4, 2)$ are isomorphic. As we see, the only example, except for the type $(2,3)$, is $(1^n, 2)$. We treat it in the following Subsection.

6.2. The Fomin-Kirillov algebras.

Let $X = \mathcal{O}_2^m$ be the rack of transpositions in $\mathbb{S}_m$, $m \geq 3$. As shown in [**MS**], see also [**AFZ**], there are two cocycles $\mathbf{q} \in Z^2(X, \mathbb{C}^\times)$ arising from Yetter-Drinfeld modules over $\mathbb{C}\mathbb{S}_m$ and such that $\mathbf{q}_{ii} = -1$ for all (some) $i \in X$. These are either $\mathbf{q} = -1$ or $\mathbf{q} = \chi$, the cocycle given by $\chi(\sigma, \tau) = \begin{cases} 1, & \text{if } \sigma(i) < \sigma(j) \\ -1, & \text{if } \sigma(i) > \sigma(j). \end{cases}$, if τ, σ are transpositions, $\tau = (ij)$ and $i < j$. Furthermore, their classes in $Z^2(X, \mathbb{C}^\times)$ are different. Hence, we have a monomorphism $\mathbb{C}^\times \times \mathbb{G}_2 \hookrightarrow H^2(\mathcal{O}_2^m, \mathbb{C}^\times)$.

Question 6. *Is $H^2(\mathcal{O}_2^m, \mathbb{C}^\times) \simeq \mathbb{C}^\times \times \mathbb{G}_2$ for $m \geq 4$?*

We conjecture that the answer is yes; Proposition 3.7 (b) gives some computational support to this conjecture, and Proposition 3.2 should be useful for this.

We turn now to the Nichols algebras associated to $X = \mathcal{O}_2^m$.

- ⋄ If $\mathbf{q} \in Z^2(X, \mathbb{C}^\times)$ arises from a Yetter-Drinfeld module over $\mathbb{C}\mathbb{S}_m$ and $\mathbf{q}_{ii} \neq -1$, then $\dim \mathfrak{B}(X, \mathbf{q}) = \infty$ [**AFZ**, Theorem 1]. In fact, assume that $m \geq 4$. Then it can be shown that $\dim \mathfrak{B}(X, \mathbf{q}) = \infty$ for any $\mathbf{q} \in \mathbb{C}^\times \times \mathbb{G}_2 \hookrightarrow H^2(\mathcal{O}_2^m, \mathbb{C}^\times)$ such that $\mathbf{q}_{ii} \neq -1$, just looking at the abelian subrack $\{(12), (34)\}$.
- ⋄ The Nichols algebras $\mathfrak{B}(\mathcal{O}_2^m, -1)$ and $\mathfrak{B}(\mathcal{O}_2^m, \chi)$ are finite-dimensional for $m = 3, 4, 5$, see Table 6. Indeed, the Hilbert series of $\mathfrak{B}(\mathcal{O}_2^m, -1)$ and $\mathfrak{B}(\mathcal{O}_2^m, \chi)$ are equal.

- ⋄ The quadratic Nichols algebra of a braided vector space V is $\widehat{\mathfrak{B}}_2(V) = T(V)/\langle \ker Q_2 \rangle$, cf. (6); clearly, here is an epimorphism $\widehat{\mathfrak{B}}_2(V) \to \mathfrak{B}(V)$. The Nichols algebras $\mathfrak{B}(\mathcal{O}_2^m, -1)$ and $\mathfrak{B}(\mathcal{O}_2^m, \chi)$ are quadratic for $m = 3, 4, 5$. Furthermore, $\mathfrak{B}(\mathcal{O}_2^m, \chi)$ appears in [**FK**] in relation with the quantum cohomology of the flag variety.
- ⋄ It is known neither if the Nichols algebras $\mathfrak{B}(\mathcal{O}_2^m, -1)$ and $\mathfrak{B}(\mathcal{O}_2^m, \chi)$ are finite-dimensional, nor if they are quadratic, for $m \geq 6$.

Question 7. *Are the cocycles -1 and χ equivalent by twist? Recall that $H^2(\mathbb{S}_m, \mathbb{C}^\times) \simeq \mathbb{Z}/2$* [**Schur**].

A positive answer to Question 7 would explain the similarities between the Nichols algebras $\mathfrak{B}(\mathcal{O}_2^m, -1)$ and $\mathfrak{B}(\mathcal{O}_2^m, \chi)$.

6.3. Sporadic groups.
The sporadic groups with non-trivial outer automorphisms group are M_{12}, M_{22}, J_2, Suz, HS, McL, He, Fi_{22}, Fi'_{24}, $O'N$, J_3, T and HN. For any group L among these, the outer automorphisms group is $\mathbb{Z}/2$ and $\mathrm{Aut}(L) \simeq L \rtimes \mathbb{Z}/2$. Hence we need to consider the conjugacy classes in $\mathrm{Aut}(L) - L$.

Theorem 6.2. [**FV**] *Let G be one of the following sporadic simple groups: M_{12}, M_{22}, J_2, Suz, HS, McL, He, $O'N$, J_3 or T. If $\mathcal{O}$ is the conjugacy class of a non-trivial element in $\mathrm{Aut}(G) - G$ NOT listed in Table 3, then $\mathcal{O}$ is of type D.* □

TABLE 3. Twisted conjugacy classes not known of type D

Group	$\mathrm{Aut}(M_{22})$	$\mathrm{Aut}(J_3)$	$\mathrm{Aut}(HS)$	$\mathrm{Aut}(McL)$	$\mathrm{Aut}(ON)$
Classes	2A	34A, 34B	2C	22A, 22B	38A, 38B, 38C

The groups $\mathrm{Aut}(Fi_{22})$, $\mathrm{Aut}(Fi'_{24})$ and $\mathrm{Aut}(HN)$ are being object of present study, see [**FV**].

7. On twisted homogeneous racks

In this section, we fix a simple non-abelian group L, an integer $t > 1$ and $\theta \in \mathrm{Out}(L)$; by abuse of notation, we call also by θ a representant in $\mathrm{Aut}(L)$. The representant of the trivial element is chosen as the trivial automorphism. Let $u \in \mathrm{Aut}(L^t)$ act by

$$u(\ell_1, \dots, \ell_t) = (\theta(\ell_t), \ell_1, \dots, \ell_{t-1}), \quad \ell_1, \dots, \ell_t \in L.$$

The twisted conjugacy class of $(x_1, \dots, x_t) \in L^t$ is called a *twisted homogeneous rack* of class (L, t, θ) and denoted $\mathcal{C}_{(x_1,\dots,x_t)}$. Let also $\mathcal{C}_\ell := \mathcal{C}_{(e,\dots,e,\ell)}$, $\ell \in L$. The set of twisted homogeneous racks of class (L, t, θ) is parameterized by the set of twisted conjugacy classes of L under θ [**AFGaV**, Prop. 3.3]. Namely,

(1) If $(x_1, \dots, x_t) \in L^t$ and $\ell = x_t x_{t-1} \cdots x_2 x_1$, then $\mathcal{C}_{(x_1,\dots,x_t)} = \mathcal{C}_\ell$.
(2) $\mathcal{C}_\ell = \mathcal{C}_k$ iff $k \in \mathcal{O}_\ell^{L,\theta}$; hence

$$\mathcal{C}_\ell = \{(x_1, \dots, x_t) \in L^t : \ x_t x_{t-1} \cdots x_2 x_1 \in \mathcal{O}_\ell^{L,\theta}\}.$$

In [**AFGaV**], we have developed some techniques to check whether $\mathcal{C}_\ell$ is of type D; so far, these techniques are more useful in the case $\theta = \mathrm{id}$. For illustration, we quote:

- If $\ell \in L$ is quasi-real of type j, $t \geq 3$ or $t = 2$ and $\mathrm{ord}(\ell) \nmid 2(1-j)$, then $\mathcal{C}_\ell$ is of type D.
- If ℓ is an involution and $t > 4$ is even, then $\mathcal{C}_\ell$ is of type D.
- If ℓ is an involution, t is odd and $\mathcal{O}_\ell^L$ is of type D, then so is $\mathcal{C}_\ell$.
- If $(t, |L|)$ is divisible by an odd prime p, or if $(t, |L|)$ is divisible by $p = 2$ and $t \geq 6$, then $\mathcal{C}_e$ is of type D.
- If $L = \mathbb{A}_5$ or $\mathbb{A}_6$ and $t = 2$, then $\mathcal{C}_e$ is not of type D (checked with GAP).

In other words, at least when $\theta = \mathrm{id}$, the worse cases are either when ℓ is an involution and $t = 2, 4$, or else when $\ell = e$.

As an application of these techniques, we have the following result.

Theorem 7.1. [**AFGaV**] *Let L be $\mathbb{A}_n$, $n \geq 5$, or a sporadic group, $t \geq 2$ and $\ell \in L$. If $\mathcal{C}_\ell$ is a twisted homogeneous rack of class (L, t, id) not listed in Tables 4 and 5, then $\mathcal{C}_\ell$ is of type D.* □

TABLE 4. THR $\mathcal{C}_\ell$ of type $(\mathbb{A}_n, t, \theta)$, $\theta = \mathrm{id}$, $t \geq 2$, $n \geq 5$, not known of type D. Those not of type D are in bold.

n	ℓ	Type of ℓ	t
any	e	(1^n)	odd, $(t, n!) = 1$
5		$(\mathbf{1^5})$	$\mathbf{2}$
5		(1^5)	4
6		$(\mathbf{1^6})$	$\mathbf{2}$
5	involution	$(1, 2^2)$	4, odd
6		$(1^2, 2^2)$	odd
8		(2^4)	odd
any	order 4	$(1^{r_1}, 2^{r_2}, 4^{r_4})$, $r_4 > 0$, $r_2 + r_4$ even	2

TABLE 5. THR $\mathcal{C}_\ell$ of type (L, t, θ), with L a sporadic group, $\theta = \mathrm{id}$, not known of type D.

sporadic	t	**Type of ℓ or class name of $\mathcal{O}_\ell^L$**
any	$(t, \|L\|) = 1$, t odd	1A
	2	$\mathrm{ord}(\ell) = 4$
T, J_2, Fi_{22}, Fi_{23}, Co_2	odd	2A
B	odd	2A, 2C
Suz	any	6B, 6C

8. Applications to the classification of pointed Hopf algebras

We say that a finite group G *collapses* if for any finite-dimensional pointed Hopf algebra H, with $G(H) \simeq G$, necessarily $H \simeq \mathbb{C}G$. Some applications of the results on Nichols algebras presented here to the classification of Hopf algebras need the following Lemma.

Lemma 8.1. [**AFGV1**, Lemma 1.4] *The following statements are equivalent:*

(1) *If* $0 \neq V \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$*, then* $\dim \mathfrak{B}(V) = \infty$.
(2) *If* $V \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$ *is* irreducible*, then* $\dim \mathfrak{B}(V) = \infty$.
(3) *G collapses.* □

Theorem 8.2. [**AFGV1, AFGV2**] *Let G be either an alternating group $\mathbb{A}_m$, $m \geq 5$, or a sporadic simple group, different from the Fischer group Fi_{22}, the Baby Monster B and the Monster M. Then G collapses.* □

The proof goes as follows: by the Lemma 8.1, we need to show that $\dim \mathfrak{B}(V) = \infty$ for any irreducible $V = M(\mathcal{O}, \rho)$. IF $\mathcal{O}$ is of type D, this follows from Theorem 2.4; and we know those classes of type D by Theorems 5.1, 5.2. The remaining pairs $(\mathcal{O}, \rho)$ are treated by abelian techniques, namely one finds an abelian subrack, computes the corresponding diagonal braiding arising from ρ and applies [**H2**].

However, there are finite non-abelian groups that do not collapse. Furthermore, the classification of all finite-dimensional pointed Hopf algebras with group G is known, when $G = \mathbb{S}_3$, $\mathbb{S}_4$ or $\mathbb{D}_{4t}$, $t \geq 3$, see [**AHS, GG, FG**], respectively.

Appendix A. Examples of finite-dimensional Nichols algebras

We now list several examples of pairs $(X, \mathbf{q})$ such that $\dim \mathfrak{B}(X, \mathbf{q}) < \infty$; we give the dimension, the top degree and the reference where the example appeared[3].

Appendix B. Questions

Question 1. *Determine all simple racks of type D.*

Question 2. *For any finite indecomposable rack X, for any $n \in \mathbb{N}$, and for any $\mathbf{q} \in H^2(X, \mathbf{GL}(n, \mathbb{C}))$, determine if* $\dim \mathfrak{B}(X, \mathbf{q}) < \infty$.

Question 3. *If X collapses at 1, does necessarily X collapse?*

Question 4. *Compute all cocycles $\mathbf{q} \in Z^2(X, \mathbb{C}^\times)$ such that $\mathbf{q}_{ii} = -1$.*

Question 5. *Is $H^2(\mathcal{O}_2^m, \mathbb{C}^\times) \simeq \mathbb{C}^\times \times \mathbb{G}_2$ for $m \geq 4$?*

Question 6. *Find the proper subracks of* Q.

[3]The Nichols algebra corresponding to $\mathsf{Q}_{\mathbb{Z}/5,2}$ was actually computed by Matías Graña. The quadratic Nichols algebra corresponding to $\mathcal{O}_2^5$ was computed by Jan-Erik Roos; Graña showed that this is a Nichols algebra. The computation of the Nichols algebras corresponding to $(\mathcal{O}_2^n, \chi)$, $n = 4, 5$, was done in [**GG**] using Deriva with the help of M. Graña.

TABLE 6. Finite-dimensional $\mathfrak{B}(X, \mathbf{q})$

X	**rk**	**q**	**Relations**	$\dim \mathfrak{B}(V)$	**top**	**Ref.**
$\mathcal{D}_3$	3	-1	5 in degree 2	$12 = 3.2^2$	$4 = 2^2$	[**MS**]
$\mathcal{T}$	4	-1	8 in degree 2, 1 in degree 6	72	$9 = 3^2$	[**G1**]
$\mathsf{Q}_{\mathbb{Z}/5,2}$	5	-1	10 in degree 2, 1 in degree 4	$1280 = 5.4^4$	$16 = 4^2$	[**AG**]
$\mathsf{Q}_{\mathbb{Z}/5,3}$	5	-1	10 in degree 2, 1 in degree 4	$1280 = 5.4^4$	$16 = 4^2$	dual of the preceding
$\mathcal{O}_2^4$	6	-1	16 in degree 2	$576 = 24^3$	12	[**FK, MS**]
$\mathcal{O}_2^4$	6	χ	16 in degree 2	$576 = 24^3$	12	[**GG**]
$\mathcal{O}_4^4$	6	-1	16 in degree 2	$576 = 24^3$	12	[**AG**]
$\mathsf{Q}_{\mathbb{Z}/7,3}$	7	-1	21 in degree 2, 1 in degree 6	$326592 = 7.6^6$	$36 = 6^2$	[**G2**]
$\mathsf{Q}_{\mathbb{Z}/7,5}$	7	-1	21 in degree 2, 1 in degree 6	$326592 = 7.6^6$	$36 = 6^2$	dual of the preceding
$\mathcal{O}_2^5$	10	-1	45 in degree 2	8294400	40	[**FK, G2**]
$\mathcal{O}_2^5$	10	χ	45 in degree 2	8294400	40	[**GG**]

Question 7. *Are the cocycles -1 and χ equivalent by twist? Recall that $H^2(\mathbb{S}_m, \mathbb{C}^\times) \simeq \mathbb{Z}/2$* [**Schur**].

Acknowledgements. N. A., G. A. G. and L. V. want to thank the Organizing Committee the invitation to attend to the *XVIII Coloquio Latinoamericano de Álgebra* and the warm hospitality in São Pedro during the Colloquium. Specially, G. A. G. thanks the invitation to give the mini-curse "Quantum Groups and Hopf Algebras".

References

[A] N. Andruskiewitsch, *About finite dimensional Hopf algebras*, Notes of a course given at the CIMPA School "Quantum symmetries in theoretical physics and mathematics", Bariloche 2000. Contemp. Math **2**94 (2002), 1–57.

[AF1] N. Andruskiewitsch and F. Fantino, *On pointed Hopf algebras associated with unmixed conjugacy classes in $\mathbb{S}_m$*, J. Math. Phys. **48** (2007), 033502-1–26.

[AF2] ______, *On pointed Hopf algebras associated with alternating and dihedral groups*, Rev. Unión Mat. Argent. **48-3** (2007), 57–71.

[AF3] ______, *New techniques for pointed Hopf algebras*, Contemp. Math. 491 (2009), 323-348.

[AFGV1] N. Andruskiewitsch, F. Fantino, M. Graña and L. Vendramin, *Finite-dimensional pointed Hopf algebras with alternating groups are trivial*. arXiv:0812.4628, Ann. Mat. Pura Appl. (4), to appear.

[AFGV2] ———, *Pointed Hopf algebras over the sporadic groups*. arXiv:1001.1108, submitted.

[AFGV3] ———, *The logbook of pointed Hopf algebras over the sporadic simple groups*. arXiv:1001.1113, submitted.

[AFGaV] N. Andruskiewitsch, F. Fantino, G. A. García and L. Vendramin, *On Twisted homogeneous racks of type D*, submitted.

[AFZ] N. Andruskiewitsch, F. Fantino and S. Zhang, *On pointed Hopf algebras associated with the symmetric groups*, Manuscripta Math. **128** (2009), 359–371.

[AG] N. Andruskiewitsch and M. Graña, *From racks to pointed Hopf algebras*, Adv. Math. **178** (2003), 177 – 243.

[AHS] N. Andruskiewitsch, I. Heckenberger and H.-J. Schneider, *The Nichols algebra of a semisimple Yetter-Drinfeld module*, Amer. J. Math., to appear.

[AS1] N. Andruskiewitsch and H.-J. Schneider, *Finite quantum groups and Cartan matrices*. Adv. Math **54** (2000), 1–45.

[AS2] ———, *Pointed Hopf Algebras*, in "New directions in Hopf algebras", 1–68, Math. Sci. Res. Inst. Publ. **43**, Cambridge Univ. Press, 2002.

[AS3] ———, *On the classification of finite-dimensional pointed Hopf algebras*, Ann. Math. **171** (2010), 375–417.

[AZ] N. Andruskiewitsch and S. Zhang, *On pointed Hopf algebras associated to some conjugacy classes in $\mathbb{S}_n$*, Proc. Amer. Math. Soc. **135** (2007), no. 9, 2723–2731.

[Ang] I. Angiono, *On Nichols algebras with standard braiding*, Algebra and Number Theory Vol. 3, No. **1** (2009), 35-106.

[Ar] E. Artin, *Theory of braids*, Ann. Math. **48** (1947), 101–126.

[Bi] J. S. Birman, *Braids, links and mapping class groups*, Princeton Univ. Press (1975).

[Bo] A. Borel, *Linear algebraic groups*, Second edition, Graduate Texts in Mathematics, **126**, Springer-Verlag, New York, 1991. xii+288 pp.

[B] N. Bourbaki, *Groupes et algèbres de Lie Chap. IV, V, VI*, Hermann, Paris, 1968.

[Bk] E. Brieskorn, *Automorphic sets and singularities*, Contemp. Math. **78** (1988), 45–115.

[DT] Y. Doi and M. Takeuchi, *Multiplication alteration by two-cocycles. The quantum version*, Commun. Algebra **22**, No.14 (1994), 5715-5732.

[D] V. Drinfeld, *Quasi-Hopf algebras*, Leningrad Math. J. **1** (1990), 1419–1457.

[EGñ] P. Etingof and M. Graña, *On rack cohomology*, J. of Pure and Applied Algebra, **177** (2003), 49–59.

[ESS] P. Etingof, T. Schedler and A. Soloviev, *Set-theoretical solutions to the Quantum Yang–Baxter Equation*, Duke Math. J. **100** (1999), 169–209.

[F] F. Fantino, *On pointed Hopf algebras associated with Mathieu groups*, J. Algebra Appl. **8** 5 (2009) 633–672.

[FG] F. Fantino and G. A. García, *On pointed Hopf algebras over dihedral groups*. In preparation.

[FV] F. Fantino and L. Vendramin, *On twisted conjugacy classes in sporadic groups of type D*. In preparation.

[FR] R. Fenn and C. Rourke, *Racks and links in codimension two*, J. Knot Theory Ramifications **1** 4 (1992), 343–406.

[FK] S. Fomin and K. N. Kirillov, *Quadratic algebras, Dunkl elements, and Schubert calculus*, Progr. Math. **172**, Birkhauser, (1999), 146–182.

[FGV1] S. Freyre, M. Graña and L. Vendramin, *On Nichols algebras over* $\mathbf{GL}(2,\mathbb{F}_q)$ *and* $\mathbf{SL}(2,\mathbb{F}_q)$, J. Math. Phys. **48** (2007), 123513-1 – 123513-11.

[FGV2] ———, *On Nichols algebras over* $\mathbf{PSL}(2,q)$ *and* $\mathbf{PGL}(2,q)$, J. Algebra Appl., Vol. 9, No. 2 (2010), 195–208.

[GAP] The GAP Group. GAP – Groups, Algorithms, and Programming, version 4.4.12, `http://www.gap-system.org`, 2008.

[GG] G. A. García and A. García Iglesias, *Finite dimensional pointed Hopf algebras over* $\mathbb{S}_4$, Israel Journal of Math., to appear, preprint: `arXiv:0904.2558v2`.

[G1] M. Graña, *On Nichols algebras of low dimension*, in "New Trends in Hopf Algebra Theory"; Contemp. Math. **267** (2000), 111–136.

[G2] ———, Finite dimensional Nichols algebras of non-diagonal group type, zoo of examples available at `\protect\vrule`width0pthttp://mate.dm.uba.ar/∼matiasg/zoo.html .

[GHV] M. Graña, I. Heckenberger and L. Vendramin, *Nichols algebras of group type with many quadratic relations*, preprint: `arXiv:1004.3723v1`.

[GV] M. Graña and L. Vendramin, *RiG, A* GAP *package for racks and Nichols Algebras*, available at `http://mate.dm.uba.ar/~lvendram`.

[H1] I. Heckenberger, *The Weyl groupoid of a Nichols algebra of diagonal type*, Invent. Math. **164** (2006), 175–188.

[H2] ———, *Classification of arithmetic root systems*, Adv. Math. **220** (2009), 59–124.

[HS] I. Heckenberger and H.-J. Schneider, *Root systems and Weyl groupoids for semisimple Nichols algebras*, `arXiv:0807.0691`. Proc. London Math. Soc., to appear.

[Hu] J.E. Humphreys, *Conjugacy classes in semisimple algebraic groups*, Mathematical Surveys and Monographs, **43**, American Mathematical Society, Providence, RI, 1995. xviii+196 pp.

[J] D. Joyce, *Simple quandles*, J. Algebra **79** 2 (1982), 307–318.

[LYZ] J.-H. Lu, M. Yan & Y. Zhu, *On Set-theoretical Yang–Baxter equation*, Duke Math. J. **104** (2000), 1–18.

[MO] S. Majid and R. Oeckl, *Twisting of Quantum Differentials and the Planck Scale Hopf Algebra*, Commun. Math. Phys. **205** (1999), 617–655.

[MS] A. Milinski and H-J. H.-J. Schneider, *Pointed Indecomposable Hopf Algebras over Coxeter Groups*, Contemp. Math. **267** (2000), 215–236.

[R] N. Reshetikhin, *Multiparameter quantum groups and twisted quasitriangular Hopf algebras*, Lett. Math. Phys. **2**0, (1990), pp. 331–335.

[Schur] I. Schur, *Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen*, Journal für die reine und angewandte Mathematik **139**, 155–250.

[S] A. Soloviev, *Non-unitary set-theoretical solutions to the quantum Yang–Baxter equation*, Math. Res. Lett. **7** (2000), no. 5-6, pp. 577–596.

[Tk] M. Takeuchi, *Survey of braided Hopf algebras*, in "New Trends in Hopf Algebra Theory"; Contemp. Math. **267** (2000), 301–324.

N. A., F. F., G. A. G.: Facultad de Matemática, Astronomía y Física, Universidad Nacional de Córdoba. CIEM – CONICET. Medina Allende s/n (5000), Ciudad Universitaria, Córdoba, Argentina

F. F., G. A. G.: Facultad de Ciencias Exactas, Físicas y Naturales, Universidad Nacional de Córdoba. Velez Sarsfield 1611 (5000), Ciudad Universitaria, Córdoba, Argentina

L. V. : Departamento de Matemática, FCEyN, Universidad de Buenos Aires, Pab. I, Ciudad Universitaria (1428), Buenos Aires, Argentina

L. V. : Instituto de Ciencias, Universidad de Gral. Sarmiento, J.M. Gutierrez 1150, Los Polvorines (1653), Buenos Aires, Argentina

E-mail address: `(andrus, fantino, ggarcia)@famaf.unc.edu.ar`

E-mail address: `lvendramin@dm.uba.ar`

On Nichols algebras associated to simple racks

N. Andruskiewitsch, F. Fantino, G. A. García, L. Vendramin

Dedicado a Matías Graña

Abstract. This is a report on the present state of the problem of determining the dimension of the Nichols algebra associated to a rack and a cocycle. This is relevant for the classification of finite-dimensional complex pointed Hopf algebras whose group of group-likes is non-abelian. We deal mainly with simple racks. We recall the notion of rack of type D, collect the known lists of simple racks of type D and include preliminary results for the open cases. This notion is important because the Nichols algebra associated to a rack of type D and any cocycle has infinite dimension. For those racks not of type D, the computation of the cohomology groups is needed. We discuss some techniques for this problem and compute explicitly the cohomology groups corresponding to some conjugacy classes in symmetric or alternating groups of low order.

1. Introduction

Throughout the paper we work over the field $\mathbb{C}$ of complex numbers. The problem of classifying finite-dimensional pointed Hopf algebras over non-abelian finite groups reduces in many cases to a question on conjugacy classes. In this introduction we give a historical account and place the problem in the overall picture.

1.1. We briefly recall the lifting method for the classification of pointed Hopf algebras, see Subsection 2.2 for unexplained terminology and [**AS2**] for a full exposition. Let H be a Hopf algebra with bijective antipode and assume that the coradical $H_0 = \sum_{C \text{ simple subcoalgebra of } H} C$ is a Hopf subalgebra of H. Consider the coradical filtration of H:

$$H_0 \subset H_1 \subset \cdots \subset H = \bigcup_{n \geq 0} H_n,$$

where $H_{i+1} = \{x \in H : \Delta(x) \in H_i \otimes H + H \otimes H_0\}$. Then the associated graded coalgebra $\operatorname{gr} H$ has a decomposition $\operatorname{gr} H \simeq R\#H_0$, where R is an algebra with

2010 *Mathematics Subject Classification.* 16T05; 17B37.

This work was partially supported by ANPCyT-Foncyt, CONICET, Ministerio de Ciencia y Tecnología (Córdoba), Secyt-UNC and Secyt-UBA.

some special properties and # stands for a kind of semidirect product (technically, a Radford biproduct or bosonization; the underlying vector space is $R \otimes H_0$). The algebra R, more precisely, is a Hopf algebra in the braided tensor category of Yetter-Drinfeld modules over H_0, see Subsection 2.2, and inherits the grading of $\operatorname{gr} H$: $R = \oplus_{n \geq 0} R^n$. If $V = R^1$, then the subalgebra of R generated by V is isomorphic to the Nichols algebra $\mathfrak{B}(V)$, that is completely determined by the Yetter-Drinfeld module V.

Let us fix a semisimple Hopf algebra A. One of the fundamental steps of the lifting method to classify finite-dimensional Hopf algebras H with $H_0 \simeq A$ is to address the following question, see [**A**]:

Question. *Determine the Yetter-Drinfeld modules V over A such that the dimension of $\mathfrak{B}(V)$ is finite, and if so, give an efficient set of relations of $\mathfrak{B}(V)$.*

An important observation is that the Nichols algebra $\mathfrak{B}(V)$, as algebra and coalgebra, is completely determined just by the braiding $c : V \otimes V \to V \otimes V$. Therefore, it is convenient to consider classes of braided vector spaces (V, c) depending on the class of semisimple Hopf algebras we are considering.

1.2. A Hopf algebra H is pointed if H_0 is isomorphic to the group algebra $\mathbb{C}G$, where G is the group of grouplikes of H. Let us consider first the case when G is abelian. A braided vector space (V, c) is of diagonal type if V has a basis $(v_i)_{1 \leq i \leq n}$ such that $c(v_i \otimes v_j) = q_{ij} v_j \otimes v_i$, where the q_{ij}'s are non-zero scalars [**AS1**]. The class of braided vector spaces of diagonal type corresponds to the class of pointed Hopf algebras with G abelian (and finite). A remarkable result is the complete list of all braided vector spaces of diagonal type with finite-dimensional Nichols algebra [**H2**]; the basic tool in the proof of this result is the Weyl groupoid [**H1**]. The classification of all finite-dimensional pointed Hopf algebras with G abelian and order of G coprime with 210 was obtained in [**AS3**], relying crucially on [**AS1, H2**]. Notice however that the article [**H2**] does not contain the efficient set of relations for finite-dimensional Nichols algebras of diagonal type; so far, this is available for the special classes of braided vector spaces of Cartan type [**AS1**] and more generally of standard type [**Ang**].

1.3. Let us now turn to the case when H is pointed with G non-abelian and mention some antecedents.

- ⋄ The first genuine examples of finite-dimensional pointed Hopf algebras with non-abelian group appeared in [**MS, FK**], as bosonizations of Nichols algebras related to the transpositions in $\mathbb{S}_3$ and $\mathbb{S}_4$, see Subsection 6.2. The analogous quadratic algebra over $\mathbb{S}_5$ was computed by Roos with a computer and proved to be a Nichols algebra in [**G2**].
- ⋄ In [**G1**], Graña identified the class of braided vector spaces corresponding to pointed Hopf algebras with non-abelian group as those constructed from racks and cocycles. He also computed in [**G2**] several finite-dimensional Nichols algebras with the help of computer programs.
- ⋄ In [**G1**], Graña also suggested to look at braided vector subspaces to decide that a Nichols algebra has infinite dimension. After [**H2**], this idea

was implemented in several papers, by looking at abelian subracks. See [**AF1, AF2, AFZ, AZ, F, FGV1, FGV2**].

- ⋄ The construction of the Weyl groupoid for braided vector spaces of diagonal type in [**H1**] was extended to braided vector spaces arising from semisimple Yetter-Drinfeld modules in [**AHS**]. This allowed to consider braided vector subspaces associated to non-abelian subracks [**AF3**]. A further study of the Weyl groupoid in [**AHS**] was undertaken in [**HS**]. An important consequence of one of the results in [**HS**] is the notion of rack of type D [**AFGV1**].

1.4. We shall explain in detail the notion of rack of type D in Subsection 2.4, but we try now to give a glimpse. As we explain in Subsection 2.2, our goal is to determine if the Nichols algebra $\mathfrak{B}(\mathcal{O},\rho)$ related to a conjugacy class $\mathcal{O}$ in a finite group G and a representation ρ of the centralizer is finite-dimensional. We say that the conjugacy class $\mathcal{O}$ is *of type D* if there exist $r, s \in \mathcal{O}$ such that

(1) $(rs)^2 \neq (sr)^2$,
(2) r is not conjugated to s in the subgroup of G generated by r, s.

Then $\dim \mathfrak{B}(\mathcal{O},\rho) = \infty$ *for any* ρ; furthermore this will happen for any group G' containing $\mathcal{O}$ as a conjugacy class (that is, as a subrack). By reasons exposed in Subsection 2.4, we focus on the following case.

Question 1. *Determine all simple racks of type D.*

The classification of finite simple racks is known, see Subsection 2.5; the list consists of conjugacy classes in groups of 3 types. In other words, we need to check, for each conjugacy class in the list of simple racks, whether there exist r, s satisfying (1) and (2) above. The main purpose of this paper is to report the actual status of this purely group-theoretical question, that is succinctly as follows.

- ⋄ [**AFGV1**] The conjugacy classes in the alternating and symmetric groups, $\mathbb{A}_m$ and $\mathbb{S}_m$, are of type D, except for a short list of exceptions listed in Theorems 5.1 and 6.1; for some of these exceptions, we know that they are not of type D, see Remark 4.2 in *loc. cit.*
- ⋄ [**AFGV2**] The conjugacy classes in the sporadic groups are of type D, except for a short list of exceptions listed in Theorems 5.2; for some of these, we know that they are not of type D, see Table 2. The verification was done with the help of GAP, see [**AFGV3**].
- ⋄ [**FV**] Twisted conjugacy classes of sporadic groups are also mostly of type D, except for a short list of exceptions, see Theorem 6.2.
- ⋄ [**AFGaV**] Some techniques to deal with twisted homogenous racks were found; so far, most of the examples dealt with are of type D.
- ⋄ We include in Subsection 5.3 some preliminary results on conjugacy classes on simple groups of Lie type; again, most of the examples are of type D.
- ⋄ The simple affine racks do not seem to be of type D.

What happens beyond type D? As we see by now, there are roughly two large classes of simple racks, one formed by the affine ones and the conjugacy class of transpositions in $\mathbb{S}_m$, and the rest. For this second class, our project is to finish

the determination of those of type D and attack the remaining ones as explained on page 8. That is, to compute the pointed sets of cocycles of degree n and then try to discard the corresponding braided vector spaces by abelian techniques. The first class is not tractable by the strategy of subracks. We should also mention the recent paper [**GHV**] with a different approach.

1.5. The paper is organized as follows. We discuss Nichols algebras, racks, cocycles, the criterion of type D, the classification of finite simple racks and the strategy of subracks in Section 2. Section 3 contains some techniques for the computation of cocycles. In the next sections we list explicitly the simple racks that are known to be of type D. In Section 8 we illustrate the consequences of these results to the classification of pointed Hopf algebras. In Appendix A, we list all known examples of finite-dimensional Nichols algebras associated to racks and cocycles; in Appendix B, we put together some questions scattered along the text.

This survey contains also a few new concepts and results, among them: the computation of the enveloping group of the rack of transpositions in $\mathbb{S}_m$, see Proposition 3.2; the twisting operation for cocycles on racks, see Subsection 3.4; the calculation of some cohomology groups using the program RiG, see Subsection 3.3; some preliminary discussions on conjugacy classes of type D in finite groups of Lie type, see Subsection 5.3.

2. Preliminaries

Conventions. $\mathbb{N} = \{1, 2, 3, \dots\}$; $\mathbb{S}_X := \{f : X \to X \text{ bijective}\}$; if $m \in \mathbb{N}$, then $\mathbb{G}_m$ is the group of m-th roots of 1 in $\mathbb{C}$.

2.1. Racks.

We briefly recall the basics of racks; see [**AG**] for more information and references. A *rack* is a pair $(X, \triangleright)$ where X is a non-empty set and $\triangleright : X \times X \to X$ is an operation such that

$$\text{the map } \varphi_x = x \triangleright \_\_ \text{ is bijective for any } x \in X, \quad \text{and} \tag{1}$$

$$x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (x \triangleright z) \text{ for all } x, y, z \in X. \tag{2}$$

A group G is a rack with $x \triangleright y = xyx^{-1}$, $x, y \in G$; if $X \subset G$ is stable under conjugation by G, that is a union of conjugacy classes, then it is a subrack of G. The main idea behind the consideration of racks is to keep track just of the conjugation of a group. Morphisms of racks and subracks are defined as usual. For instance, $\varphi : X \to \mathbb{S}_X$, $x \mapsto \varphi_x$, is a morphism of racks, for any rack X. Any rack X considered here satisfies the conditions

$$x \triangleright x = x, \tag{3}$$

$$x \triangleright y = y \implies y \triangleright x = x, \tag{4}$$

for any $x, y \in X$. This is technically a *crossed set*, but we shall simply say a rack. So, we rule out, for example, the permutation rack (X, σ), where $\sigma \in \mathbb{S}_X$ and $\varphi_x = \sigma$ for all x.

The rack with just one element is called *trivial*.

We shall consider some special classes of racks that we describe now.

Affine racks. If A is an abelian group and $T \in \mathrm{Aut}(A)$, then A is a rack with $x \triangleright y = (1 - T)x + Ty$. This is called an *affine rack* and denoted $\mathsf{Q}_{A,T}$.

Twisted conjugacy classes. Let G be a finite group and $u \in \mathrm{Aut}(G)$; G acts on itself by $x \rightharpoonup_u y = x\,y\,u(x^{-1})$, $x, y \in G$. The orbit $\mathcal{O}_x^{G,u}$ of $x \in G$ by this action is a rack with operation

$$y \triangleright_u z = y\,u(z\,y^{-1}), \quad y, z \in \mathcal{O}_x^{G,u}. \tag{5}$$

We shall say that $\mathcal{O}_x^{G,u}$ is a *twisted conjugacy class* of type (G, u).

Notation.

- $\mathcal{T}$ = any of the conjugacy classes of 3-cycles in $\mathbb{A}_4$ (the tetrahedral rack).
- $\mathsf{Q}_{A,T}$ = affine rack associated to an abelian group A and $T \in \mathrm{Aut}(A)$.
- $\mathcal{D}_n$ = class of involutions in the dihedral group of order $2n$, n odd.
- $\mathcal{O}_j^m$ = conjugacy class of j-cycles in $\mathbb{S}_m$.

We need some terminology on racks.

- A rack X is *decomposable* if it can expressed as a disjoint union of subracks $X = X_1 \coprod X_2$. Otherwise, X is *indecomposable*.
- A rack X is said to be *simple* iff $\operatorname{card} X > 1$ and for any surjective morphism of racks $\pi : X \to Y$, either π is a bijection or $\operatorname{card} Y = 1$.
- If X is a rack and $j \in \mathbb{Z}$, then $X^{[j]}$ is the rack with the same set X and multiplication $\triangleright^j$ given by $x \triangleright^j y = \varphi_x^j(y)$, $x, y \in X$.

2.2. Nichols algebras.

Nichols algebras play a crucial role in the classification of Hopf algebras, see [**AS2**] or a brief account in Section 8 below. Let $n \geq 2$ be an integer. We start by reminding the well-known presentations by generators and relations of the braid group $\mathbb{B}_n$ and the symmetric group $\mathbb{S}_n$:

$$\mathbb{B}_n = \langle (\sigma_i)_{1 \leq i \leq n-1} | \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j,\ |i-j| = 1; \quad \sigma_i\sigma_j = \sigma_j\sigma_i,\ |i-j| > 1 \rangle$$

$$\mathbb{S}_n = \langle (s_i)_{1 \leq i \leq n-1} | s_is_js_i = s_js_is_j,\ |i-j| = 1; \quad s_is_j = s_js_i,\ |i-j| > 1; \quad s_i^2 = e \rangle,$$

indices in the relations going over all possible i, j. There is a canonical projection $\pi : \mathbb{B}_n \to \mathbb{S}_n$, that admits a so-called Matsumoto section $M : \mathbb{S}_n \to \mathbb{B}_n$; this is not a morphism of groups, and it is defined by $M(s_i) = \sigma_i$, $1 \leq i \leq n-1$, and $M(st) = M(s)M(t)$, for any $s, t \in \mathbb{S}_n$ such that $l(st) = l(s) + l(t)$, l being the length of a word in generators s_i.

Let V be a vector space and $c \in \mathbf{GL}(V \otimes V)$. Recall that c fulfills the braid equation if $(c \otimes \mathrm{id})(\mathrm{id} \otimes c)(c \otimes \mathrm{id}) = (\mathrm{id} \otimes c)(c \otimes \mathrm{id})(\mathrm{id} \otimes c)$. In this case, we say that (V, c) is a *braided vector space* and that c is a *braiding*. Since c satisfies the braid equation, it induces a representation of the braid group $\mathbb{B}_n$, $\rho_n : \mathbb{B}_n \to \mathbf{GL}(V^{\otimes n})$, for each $n \geq 2$. Explicitly, $\rho_n(\sigma_i) = \mathrm{id}_{V^{\otimes(i-1)}} \otimes c \otimes \mathrm{id}_{V^{\otimes(n-i-1)}}$, $1 \leq i \leq n-1$. Let

$$Q_n = \sum_{\sigma \in \mathbb{S}_n} \rho_n(M(\sigma)) \in End(V^{\otimes n}). \tag{6}$$

Then the *Nichols algebra* $\mathfrak{B}(V)$ is the quotient of the tensor algebra $T(V)$ by $\oplus_{n \geq 2} \ker Q_n$, in fact a 2-sided ideal of $T(V)$. If $c = \tau$ is the usual switch, then $\mathfrak{B}(V)$ is just the symmetric algebra of V; if $c = -\tau$, then $\mathfrak{B}(V)$ is the exterior algebra of V. But the computation of the Nichols algebra of an arbitrary braided vector space is a delicate issue. We are interested in the Nichols algebras of the braided vector spaces arising from Yetter-Drinfeld modules[1].

[1]Any braided vector space with *rigid* braiding arises as a Yetter-Drinfeld module [**Tk**].

A *Yetter-Drinfeld module* over a Hopf algebra H with bijective antipode $\mathcal{S}$ is a left H-module M and simultaneously a left H-comodule, with coaction $\lambda : M \to H \otimes M$ compatible with the action in the sense that $\lambda(h \cdot x) = h_{(1)}x_{(-1)}\mathcal{S}(h_{(3)}) \otimes h_{(2)} \cdot x_{(0)}$, for any $h \in H$, $x \in M$. Here $\lambda(x) = x_{(-1)} \otimes x_{(0)}$, in Heyneman-Sweedler notation. A Yetter-Drinfeld module M is a braided vector space with $c(m \otimes n) = m_{(-1)} \cdot n \otimes m_{(0)}$, $m, n \in M$. We shall see in Section 8 how Nichols algebras of Yetter-Drinfeld modules enter into the classification of Hopf algebras. In this paper, we are interested in the case when $H = \mathbb{C}G$ is the group algebra of a finite group G. In this setting, a Yetter-Drinfeld module over H is a left G-module M that bears also a G-grading $M = \oplus_{g\in G} M_g$, compatibility meaning that $h \cdot M_g = M_{hgh^{-1}}$ for all $h, g \in G$; the braiding is $c(m \otimes n) = g \cdot n \otimes m$, $m \in M_g$, $n \in M$.

Now a braided vector space may be realized as a Yetter-Drinfeld module over many different groups and in many different ways. It is natural to look for a description of the class of braided vector spaces that actually arise as Yetter-Drinfeld modules over some finite group and to study them by their own. If G is a finite group, then any Yetter-Drinfeld module over the group algebra $\mathbb{C}G$ is semisimple. Furthermore, it is well-known that the set of isomorphism classes of irreducible Yetter-Drinfeld modules over $\mathbb{C}G$ is parameterized by pairs $(\mathcal{O}, \rho)$, where $\mathcal{O}$ is a conjugacy class of G and ρ is an irreducible representation of the centralizer of a fixed point in $\mathcal{O}$. M. Graña observed that the class of braided vector spaces arising from Yetter-Drinfeld modules over finite groups is described using racks and cocycles, see [**G1**] and also [**AG**, Th. 4.14].

2.3. Nichols algebras associated to racks and cocycles.

We are focused in this paper on Nichols algebras associated to braided vector spaces built from racks and cocycles. We start by describing the cocycles associated to racks. Let X be a rack and $n \in \mathbb{N}$. A map $\mathbf{q} : X \times X \to \mathbf{GL}(n, \mathbb{C})$ is a *2-cocycle* of degree n if

$$\mathbf{q}_{x,y\triangleright z}\mathbf{q}_{y,z} = \mathbf{q}_{x\triangleright y,x\triangleright z}\mathbf{q}_{x,z},$$

for all $x, y, z \in X$. Let $\mathbf{q}$ be a 2-cocycle of degree n, $V = \mathbb{C}X \otimes \mathbb{C}^n$, where $\mathbb{C}X$ is the vector space with basis e_x, for $x \in X$. We denote $e_x v := e_x \otimes v$. Consider the linear isomorphism $c^{\mathbf{q}} : V \otimes V \to V \otimes V$,

$$c^{\mathbf{q}}(e_x v \otimes e_y w) = e_{x\triangleright y}\mathbf{q}_{x,y}(w) \otimes e_x v, \tag{7}$$

$x, y \in X$, $v, w \in \mathbb{C}^n$. Then $c^{\mathbf{q}}$ is a solution of the braid equation:

$$(c^{\mathbf{q}} \otimes \mathrm{id})(\mathrm{id} \otimes c^{\mathbf{q}})(c^{\mathbf{q}} \otimes \mathrm{id}) = (\mathrm{id} \otimes c^{\mathbf{q}})(c^{\mathbf{q}} \otimes \mathrm{id})(\mathrm{id} \otimes c^{\mathbf{q}}).$$

Example 2.1. Let X be a finite rack and $\mathbf{q}$ a 2-cocycle. The dual braided vector space of $(\mathbb{C}X \otimes \mathbb{C}^n, c^{\mathbf{q}})$ is isomorphic to $(\mathbb{C}X^{[-1]} \otimes \mathbb{C}^n, c^{\widehat{\mathbf{q}}})$ where $\widehat{\mathbf{q}}_{x,y} = \mathbf{q}_{x,x\triangleright^{-1}y}$, $x, y \in X^{[-1]}$. See Subsection 2.1 for $X^{[-1]}$.

The Nichols algebra associated to $c^{\mathbf{q}}$ is denoted $\mathfrak{B}(X, \mathbf{q})$.

We need to consider only 2-cocycles (or simply cocycles, for short) with some specific properties.

- A cocycle $\mathbf{q}$ is *finite* if its image generates a finite subgroup of $\mathbf{GL}(n, \mathbb{C})$.
- A cocycle $\mathbf{q}$ is *faithful* if the morphism of racks $g : X \to \mathbf{GL}(V)$ defined by $g_x(e_y w) = e_{x\triangleright y}\mathbf{q}_{x,y}(w)$, $x, y \in X$, $w \in V$, is injective.

We denote by $Z^2(X, \mathbf{GL}(n,\mathbb{C}))$ the set of all finite faithful 2-cocycles of degree n. Let $\mathbf{q} \in Z^2(X, \mathbf{GL}(n,\mathbb{C}))$ and $\gamma : X \to \mathbf{GL}(n,\mathbb{C})$ a map whose image generates a finite subgroup. Define $\widetilde{\mathbf{q}} : X \times X \to \mathbf{GL}(n,\mathbb{C})$

$$\widetilde{\mathbf{q}}_{ij} = (\gamma_{i \triangleright j})^{-1}\, \mathbf{q}_{ij} \gamma_j. \tag{8}$$

Then $\widetilde{\mathbf{q}}$ is also a finite faithful cocycle and "$\mathbf{q} \sim \widetilde{\mathbf{q}}$ iff they are related by (8) for some γ" defines an equivalence relation. We set

$$H^2(X, \mathbf{GL}(n,\mathbb{C})) = Z^2(X, \mathbf{GL}(n,\mathbb{C}))/\sim. \tag{9}$$

If $\mathbf{q} \sim \widetilde{\mathbf{q}}$, then the Nichols algebras $\mathfrak{B}(X, \mathbf{q})$ and $\mathfrak{B}(X, \widetilde{\mathbf{q}})$ are isomorphic as braided Hopf algebras in the sense of [**Tk**], see [**AG**, Th. 4.14]. The converse is not true, see [**G1**].

The main question we want to solve is the following.

Question 2. *For any finite indecomposable rack X, for any $n \in \mathbb{N}$, and for any $\mathbf{q} \in H^2(X, \mathbf{GL}(n,\mathbb{C}))$, determine if $\dim \mathfrak{B}(X, \mathbf{q}) < \infty$.*

Definition 2.2. An indecomposable finite rack X *collapses at n* if for any finite faithful cocycle $\mathbf{q}$ of degree n, $\dim \mathfrak{B}(X, \mathbf{q}) = \infty$; X *collapses* if it collapses at n for any $n \in \mathbb{N}$.

The first idea that comes to the mind is one would need to compute the group $H^2(X, \mathbf{GL}(n,\mathbb{C}))$ for any n. We shall see that in many cases this is actually not necessary.

Question 3. *If X collapses at 1, does necessarily X collapse?*

Even partial answers to Question 3 would be very interesting.

2.4. Racks of type D.

We now turn to a setting where the calculation of the cocycles is not needed.

Definition 2.3. Let $(X, \triangleright)$ be a rack. We say that X is *of type D* if there exists a decomposable subrack $Y = R \coprod S$ of X such that

$$r \triangleright (s \triangleright (r \triangleright s)) \neq s, \quad \text{for some } r \in R, s \in S. \tag{10}$$

The following important result is a consequence of [**HS**, Th. 8.6], proved using the main result of [**AHS**].

Theorem 2.4. [**AFGV1**, Th. 3.6] *If X is a finite rack of type D, then X collapses.* □

Therefore, it is very important to determine all simple racks of type D, formally stated as Question 1. The classification of simple racks is known and will be evoked below. We focus on simple racks because of the following reasons:

- If Z is a finite rack and admits a rack epimorphism $\pi : Z \to X$, where X is of type D, then Z is of type D.
- If Z is indecomposable, then it admits a rack epimorphism $\pi : Z \to X$ with X simple.

We collect some criteria on racks of type D, see [**AFGV1**, Subsection 3.2].

- If $Y \subseteq X$ is a subrack of type D, then X is of type D.
- If X is of type D and Z is a rack, then $X \times Z$ is of type D.
- Let K be a subgroup of a finite group G and $\kappa \in C_G(K)$. Let $\mathcal{R}_\kappa : K \to G$ be the map given by $g \mapsto \widetilde{g} := g\kappa$. Let $\mathcal{O}$, resp. $\widetilde{\mathcal{O}}$, be the conjugacy class of $\tau \in K$, resp. of $\widetilde{\tau}$ in G. Then $\mathcal{R}_\kappa$ identifies $\mathcal{O}$ with a subrack of $\widetilde{\mathcal{O}}$. Hence, if $\mathcal{O}$ is of type D, then $\widetilde{\mathcal{O}}$ is of type D.

There is a variation of the last criterium that needs the notion of *quasi-real* conjugacy class. Let G be a finite group, $g \in G$ and $j \in \mathbb{N}$. Recall that $\mathcal{O}_g^G$ is quasi-real of type j if $g^j \neq g$ and $g^j \in \mathcal{O}_g^G$. If g is real, that is $g^{-1} \in \mathcal{O}_g^G$, but not an involution, then $\mathcal{O}_g^G$ is quasi-real of type $\operatorname{ord}(g) - 1$.

Proposition 2.5. [**AFGV1**, Ex. 3.8] *Let G be a finite group and $g = \tau\kappa \in G$, where $\tau \neq e$ and $\kappa \neq e$ commute. Let $K = C_G(\kappa) \ni \tau$; then $\kappa \in C_G(K)$. Hence, the conjugacy class $\mathcal{O}$ of τ in K can be identified with a subrack of the conjugacy class $\widetilde{\mathcal{O}}$ of g in G via $\mathcal{R}_\kappa$ as above. Assume that*

(1) *$\widetilde{\mathcal{O}}$ and $\mathcal{O}$ are quasi-real of type j,*
(2) *the orders N of τ and M of κ are coprime,*
(3) *M does not divide $j - 1$,*
(4) *there exist r_0, $s_0 \in \mathcal{O}$ such that $r_0 \triangleright (s_0 \triangleright (r_0 \triangleright s_0)) \neq s_0$.*

Then $\widetilde{\mathcal{O}}$ is of type D. $\square$

2.5. Simple racks.
Finite simple racks have been classified in [**AG**, Th. 3.9, Th. 3.12]– see also [**J**]. Explicitly, any simple rack falls into one and only one of the following classes:

(1) *Simple affine racks* $(\mathbb{F}_p{}^t, T)$, where p a prime, $t \in \mathbb{N}$, and T is the companion matrix of a monic irreducible polynomial $f \in \mathbb{F}_p[\mathtt{X}]$ of degree t, different from $\mathtt{X}$ and $\mathtt{X} - \mathtt{1}$.
(2) *Non-trivial (twisted) conjugacy classes in simple groups.*
(3) *Simple twisted homogeneous racks*, that is twisted conjugacy classes of type (G, u), where
   - $G = L^t$, with L a simple non-abelian group and $1 < t \in \mathbb{N}$,
   - $u \in \operatorname{Aut}(L^t)$ acts by
   $$u(\ell_1, \dots, \ell_t) = (\theta(\ell_t), \ell_1, \dots, \ell_{t-1}), \quad \ell_1, \dots, \ell_t \in L,$$
   for some $\theta \in \operatorname{Aut}(L)$. Furthermore, L and t are unique, and θ only depends on its conjugacy class in $\operatorname{Out}(L^t)$.

Notation. A *simple rack of type* (L, t, θ) is a twisted homogeneous rack as in (3).

2.6. The approach by subracks.
The experience shows that the following strategy is useful to approach the study of Nichols algebras over finite groups. However, there are racks that can not be treated in this way.

Strategy. *Let X be a simple rack.*

Step 1: *Is X of type D? In the affirmative, we are done: X and any indecomposable rack Z that admits a rack epimorphism $Z \to X$ collapse, in the sense of Definition 2.2.*

Step 2: *If not, look for the abelian subracks of X. For an abelian subrack S and any $\mathbf{q} \in H^2(X, \mathbb{C}^\times)$, look at the diagonal braiding with matrix $(\mathbf{q}_{ij})_{i,j\in S}$. If the Nichols algebra associated to this diagonal braiding has infinite dimension, and this is known from* [**H2**]*, then so has $\mathfrak{B}(X, \mathbf{q})$. Here you do not need to know all the abelian subracks, just to find one with the above condition.*

Step 3: *Extend the analysis of Step 2 to cocycles of arbitrary degree.*

Step 4: *Extend the analysis of Steps 2 and 3 to indecomposable racks Z that admit a rack epimorphism $Z \to X$.*

The following algorithm is the tool needed to deal with Step 1, when the rack X is realized as a conjugacy class.

Algorithm. *Let Γ be a finite group and let $\mathcal{O}$ be a conjugacy class. Fix $r \in \mathcal{O}$.*

(1) *For any $s \in \mathcal{O}$, check if $(rs)^2 \neq (sr)^2$; this is equivalent to* (10).

(2) *If such s is found, consider the subgroup H generated by r, s. If $\mathcal{O}_r^H \cap \mathcal{O}_s^H = \emptyset$, then $Y = \mathcal{O}_r^H \coprod \mathcal{O}_s^H$ is the decomposable subrack we are looking for and $\mathcal{O}$ is of type D.*

In practice, we implement this algorithm in a recursive way, running over the maximal subgroups, see [**AFGV2**] for details.

Let X be a rack and S a subset of X. We denote $\ll S \gg := \bigcap_{\substack{Y \text{subrack}, \\ S\subset Y\subset X}} Y$. If X is a subrack of a group G and $H = \langle S \rangle$, then $\ll S \gg = \bigcup_{s\in S} \mathcal{O}_s^H$.

There are racks that could not be dealt with the criterium of type D.

Definition 2.6. An indecomposable finite rack X is *of type M* if[2] for any $r, s \in X$, $\ll\{r,s\}\gg$ either is indecomposable or else equals $\{r, s\}$.

There are racks such that all proper subracks are abelian; for instance, the conjugacy class of type $(2, 3)$ in $\mathbb{S}_5$ (here, all proper subracks have at most 2 elements). More examples of racks of type M can be found in [**AFGV1**, Remark 4.2].

3. Tools for cocycles

3.1. The enveloping group.

The enveloping group $\mathbb{G}_X := \langle e_x : x \in X | e_x\, e_y = e_{x\triangleright y}\, e_x, x, y \in X\rangle$ was introduced in [**Bk, FR, J**]; it was also considered in [**LYZ, ESS, S**]. The map $e : X \to \mathbb{G}_X$, $x \mapsto e_x$ has a universal property:

If H is a group and $f : X \to H$ is a morphism of racks, then there is a unique morphism of groups $F : \mathbb{G}_X \to H$ such that $F(e_x) = f_x$, $x \in X$.

[2] M stands for Montevideo, where this notion was discussed by two of the authors.

In other words, $X \rightsquigarrow \mathbb{G}_X$ is the adjoint of the forgetful functor from groups to racks.

Since $\varphi : X \to \mathbb{S}_X$ is a morphism of racks, there is a group morphism $\Phi : \mathbb{G}_X \to \mathbb{S}_X$. The image, resp. the kernel, of Φ is denoted $\operatorname{Inn}_\triangleright(X)$ (the group of inner automorphisms), resp. Γ_X (the defect group).

The group $\operatorname{Inn}_\triangleright(X)$ is not difficult to compute in the case of our interest. As for the defect group, some properties were established by Soloviev.

Theorem 3.1. (a) *If X is a subrack of a group H, then $\operatorname{Inn}_\triangleright(X) \simeq C/Z(C)$, where C is the subgroup generated by X* [**AG**, Lemma 1.9].

(b) *The defect group Γ_X is central in $\mathbb{G}_X$* [**S**, Th. 2.6]. *Hence $\Gamma_X = Z(\mathbb{G}_X)$ if $\operatorname{Inn}_\triangleright(X)$ is centerless.*

(c) *The rank of Γ_X is the number of $\operatorname{Inn}_\triangleright(X)$-orbits in X* [**S**, Th. 2.10]. $\square$

The difficult part of the calculation of the defect group is to compute its torsion.

Proposition 3.2. *Let $s_i = (i\, i+1) \in \mathbb{S}_m$. Let X be the rack of transpositions in $\mathbb{S}_m$; this is the conjugacy class of s_1. The enveloping group $\mathbb{G}_X$ of X is a central extension*

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{G}_X \longrightarrow \mathbb{S}_m \longrightarrow 0 \tag{11}$$

Proof. By property (a) above, $\operatorname{Inn}_\triangleright(X) \simeq \mathbb{S}_m$. We have to compute Γ_X. Let $\mathbb{B}_m$ be the braid group and as in Subsection 2.2; let $\mathbb{P}_m = \ker \pi$, the pure braid group. We claim that there is a morphism of groups $\Psi : \mathbb{B}_m \to \mathbb{G}_X$ with $\Psi(\sigma_i) = e_{s_i}$, $1 \le i \le m-1$. To prove the claim, we verify the defining relations of the braid group:

$$\text{If } |i-j| \ge 2, \text{ then} \qquad e_{s_i} e_{s_j} = e_{s_i \triangleright s_j} e_{s_i} = e_{s_j} e_{s_i};$$

$$\text{if } |i-j| = 1, \text{ then} \qquad e_{s_i} e_{s_j} e_{s_i} = e_{s_i} e_{s_j \triangleright s_i} e_{s_j} = e_{s_i \triangleright (s_j \triangleright s_i)} e_{s_i} e_{s_j} = e_{s_j} e_{s_i} e_{s_j}$$

since $s_i \triangleright (s_j \triangleright s_i) = s_j$ in $\mathbb{S}_m$. In other words, we have a commutative diagram

$$\begin{tikzcd} \mathbb{B}_m \arrow[rr, "\Psi"] \arrow[dr, "\pi"'] & & \mathbb{G}_X \arrow[dl, "\Phi"] \\ & \mathbb{S}_m. & \end{tikzcd}$$

Clearly, Ψ is surjective and $\ker \Phi = \Psi(\mathbb{P}_m)$. Let now H be a group and $f : X \to H$ a morphism of racks. If $x, y \in X$, then $f_x^2 f_y = f_x f_{x \triangleright y} f_x = f_y f_x^2$ and consequently $f_{y \triangleright x}^2 = f_y f_x^2 f_y^{-1} = f_x^2$. Hence for all $x, y \in X$,

$$f_y^2 = f_x^2 \quad \text{is central in the subgroup generated by } f(X). \tag{12}$$

We call $z = e_{s_i}^2$; this is a central element of $\mathbb{G}_X$ and does not depend on i. Now $\mathbb{P}_m$ is generated by $\tau_{ij} = \sigma_j \triangleright (\sigma_{j+1} \triangleright (\sigma_{j+2} \triangleright \dots \triangleright (\sigma_{i-1} \triangleright \sigma_i^2))$ for all $j < i$, see [**Ar**, page 119],[**Bi**]. Hence $\ker \Phi = \Psi(\mathbb{P}_m)$ is generated by $\Psi(\tau_{ij}) = z$.

Let now V be a vector space with a basis $(v_x)_{x \in X}$ and let $q \in \mathbb{C}$ be a root of 1 of arbitrary order M. Define $f_y \in \mathbf{GL}(V)$ by $f_y(v_x) = q v_{y \triangleright x}$, $x, y \in X$. Then $f_x f_y =$

$f_{x\triangleright y} f_x$ and $f_x^2 = q^2\,\mathrm{id}$ for any $x, y \in X$; thus we have a map $F : \mathbb{G}_X \to \mathbf{GL}(V)$ and $F(z) = q^2\,\mathrm{id}$. This implies that z is not torsion and the claim is proved. □

Remark 3.3. (i). By [**B**, Ch IV, §1, no. 1.9, Prop. 5], there is a section of sets $T : \mathbb{S}_m \to \mathbb{G}_X$ such that $T(ww') = T(w)T(w')$ when $\ell(ww') = \ell(w)\ell(w')$. Thus the central extension corresponds to the cocycle $\eta : \mathbb{S}_m \times \mathbb{S}_m \to \mathbb{Z}$, $\eta(w, w') = T(w)T(w')T(ww')^{-1}$, $w, w' \in \mathbb{S}_m$.

(ii). The proof shows the centrality of Γ_X directly without referring to Theorem 3.1 (b). By Theorem 3.1 (c), z is not torsion; the last paragraph of the proof avoids appealing to this result.

Let $(X, \triangleright)$ be a rack, $\mathbf{q} : X \times X \to \mathbf{GL}(n, \mathbb{C})$ a 2-cocycle of degree n and $(V, c) = (\mathbb{C}X \otimes \mathbb{C}^n, c^{\mathbf{q}})$, *cf.* (7). We discuss how to realize (V, c) as a Yetter-Drinfeld module over a group algebra. Let $x \in X$ and define $g_x : V \to V$ by

$$g_x(e_y w) = e_{x\triangleright y}\mathbf{q}_{x,y}(w), \qquad y \in X, w \in \mathbb{C}^n, \tag{13}$$

and let $\mathrm{Inn}_{X,\mathbf{q}}$ be the subgroup of $\mathbf{GL}(V)$ generated by the g_x's, $x \in X$. Then $g_x g_y = g_{x\triangleright y} g_x$ for any $x, y \in X$, and (V, c) is a Yetter-Drinfeld module over the group algebra of $\mathrm{Inn}_{X,\mathbf{q}}$, with the natural action and coaction $\delta(e_x v) = g_x \otimes e_x v$, $x \in X$, $v \in \mathbb{C}^n$.

Lemma 3.4. *Let F be a group provided with:*

- *a group homomorphism $p : F \to \mathrm{Inn}_{X,\mathbf{q}}$;*
- *a rack homomorphism $s : X \to F$ such that $p(s_x) = g_x$ and F is generated as a group by $s(X)$.*

Then $(V, c) \in {}^{\mathbb{C}F}_{\mathbb{C}F}\mathcal{YD}$, with the action induced by p and coaction $\delta(e_x v) = s_x \otimes e_x v$, $x \in X$, $v \in \mathbb{C}^n$. In particular, $(V, c) \in {}^{\mathbb{C}\mathbb{G}_X}_{\mathbb{C}\mathbb{G}_X}\mathcal{YD}$.

Proof. If $x, y \in X$ and $w \in \mathbb{C}^n$, then $\delta(s_x \cdot e_y w) = \delta(e_{x\triangleright y}\mathbf{q}_{x,y}(w)) = s_{x\triangleright y} \otimes e_{x\triangleright y}\mathbf{q}_{x,y}(w) = s_x s_y s_x^{-1} \otimes e_{x\triangleright y}\mathbf{q}_{x,y}(w) = s_x s_y s_x^{-1} \otimes s_x \cdot w$. Since F is generated by $s(X)$, it follows that $\delta(f \cdot e_y w) = f s_y f^{-1} \otimes f \cdot w$, for all $f \in F$. □

As a consequence, the Nichols algebra of the braided vector space $(\mathbb{C}X, c_q)$ bears a $\mathbb{G}_X$-grading, that we shall call the *principal* grading, as opposed to the natural $\mathbb{N}$-grading. Indeed, if X is abelian, then $\mathbb{G}_X \simeq \mathbb{Z}^{\mathrm{card}\,X}$ and the principal grading coincides with the one considered *e. g.* in [**AHS**].

3.2. The rack cohomology group $H^2(X, \mathbb{C}^\times)$.

We now state some general facts about the cocycles on a rack X with values in the abelian group $\mathbb{C}^\times$. In this case, the H^2 is part of a cohomology theory, see [**AG**] and references therein. An alternative description of $H^2(X, \mathbb{C}^\times)$ was found in [**EGñ**] through the enveloping group. Namely, let $\mathrm{Fun}(X, \mathbb{C}^\times)$ be the space of all functions from X to $\mathbb{C}^\times$ with right $\mathbb{G}_X$-action given by $(f \cdot e_x)(y) = f(x \triangleright y)$, $f : X \to A$, $x, y \in X$.

Lemma 3.5. [**EGñ**] $H^2(X, \mathbb{C}^\times) \simeq H^1(\mathbb{G}_X, \mathrm{Fun}(X, \mathbb{C}^\times))$. □

In principle, the cohomology of $\mathbb{G}_X$ could be studied via the Hochschild-Serre sequence from that of $\mathrm{Inn}_\triangleright(X)$ and Γ_X. However, the computation of the defect group seems to be very difficult. There is also a homology theory of racks, related to the computation we are interested in by the following result.

Lemma 3.6. [**AG**, Lemma 4.7] $H^2(X,\mathbb{C}^\times) \simeq \mathit{Hom}(H_2(X,\mathbb{Z}),\mathbb{C}^\times)$. □

There is a monomorphism $\mathbb{C}^\times \hookrightarrow H^2(X,\mathbb{C}^\times)$, since any constant function is a cocycle. A natural question is to compute the quotient $H^2(X,\mathbb{C}^\times)/\mathbb{C}^\times$. *Assume that X is indecomposable.* If $\mathbf{q} \in Z^2(X,\mathbb{C}^\times)$, then

$$\mathbf{q}_{ii} = \mathbf{q}_{jj}, \quad \text{for any } i,j \in X. \tag{14}$$

Note also that $\mathbf{q} \sim \widetilde{\mathbf{q}}$ as in (8) implies that $\mathbf{q}_{ii} = \widetilde{\mathbf{q}}_{ii}$ for all $i \in X$. Therefore the question can be rephrased as follows.

Question 4. *Compute all cocycles $\mathbf{q} \in Z^2(X,\mathbb{C}^\times)$ such that $\mathbf{q}_{ii} = -1$.*

3.3. The program RiG.

A program for calculations with racks, that in particular computes the rack-(co)homology groups, was developed in [**GV**]. We use it to compute some cohomology groups of simple racks that are not of type D, see Theorems 5.1 and 6.1.

We say that $\sigma \in \mathbb{S}_n$ is of type $(1^{n_1}, 2^{n_2}, \dots, m^{n_m})$ if the decomposition of σ as product of disjoint cycles contains n_j cycles of length j, for every j, $1 \le j \le m$.

Proposition 3.7. *Let $\sigma \in \mathbb{S}_m$ be of type $(1^{n_1}, 2^{n_2}, \dots, m^{n_m})$ and let*

$$\mathcal{O} = \begin{cases} \text{the conjugacy class of } \sigma \text{ in } \mathbb{S}_m, & \text{if } \sigma \notin \mathbb{A}_m, \\ \text{the conjugacy class of } \sigma \text{ in } \mathbb{A}_m, & \text{if } \sigma \in \mathbb{A}_m. \end{cases}$$

(a) *If $m = 5$ and the type is $(2,3)$, then $H^2(\mathcal{O},\mathbb{C}^\times) = \mathbb{C}^\times \times \mathbb{G}_6$.*
(b) *If $m = 6,7,8$ and the type is $(1^n,2)$, then $H^2(\mathcal{O},\mathbb{C}^\times) = \mathbb{C}^\times \times \mathbb{G}_2$.*
(c) *If $m = 6$ and the type is (2^3), then $H^2(\mathcal{O},\mathbb{C}^\times) = \mathbb{C}^\times \times \mathbb{G}_2$.*
(d) *If $m = 5$ and the type is $(1^2,3)$, then $H^2(\mathcal{O},\mathbb{C}^\times) = \mathbb{C}^\times \times \mathbb{G}_6$.*
(e) *If $m = 6$ and the type is $(1,2,3)$, then $H^2(\mathcal{O},\mathbb{C}^\times) = \mathbb{C}^\times \times \mathbb{G}_3 \times \mathbb{G}_6$.*

TABLE 1. Some homology groups of conjugacy classes in $\mathbb{S}_m$.

type of X		$H_2(X,\mathbb{Z})$
$\mathbb{S}_5$	$(1\,2)(3\,4\,5)$	$\mathbb{Z} \oplus \mathbb{Z}/6$
$\mathbb{A}_5$	$(1\,2\,3)$	$\mathbb{Z} \oplus \mathbb{Z}/6$
$\mathbb{S}_6$	$(1\,2)(3\,4)(5\,6)$	$\mathbb{Z} \oplus \mathbb{Z}/2$
$\mathbb{S}_6$	$(1\,2)$	$\mathbb{Z} \oplus \mathbb{Z}/2$
$\mathbb{A}_6$	$(1\,2\,3)$	$\mathbb{Z} \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/6$
$\mathbb{S}_7$	$(1\,2)$	$\mathbb{Z} \oplus \mathbb{Z}/2$
$\mathbb{S}_8$	$(1\,2)$	$\mathbb{Z} \oplus \mathbb{Z}/2$

PROOF. We use GAP and RiG to compute the homology groups $H_2(\mathcal{O},\mathbb{Z})$. These results are listed in Table 1. Now assume X is a rack and that there exists $m \in \mathbb{N}_{\geq 2}$ such that $H_2(X,\mathbb{Z}) \simeq \mathbb{Z} \oplus \mathbb{Z}/m_1 \oplus \cdots \oplus \mathbb{Z}/m_r$. By Lemma 3.6, we have $H^2(X,\mathbb{C}^\times) \simeq \mathrm{Hom}(\mathbb{Z}\oplus\mathbb{Z}/m_1\oplus\cdots\oplus\mathbb{Z}/m_r,\mathbb{C}^\times) \simeq \mathrm{Hom}(\mathbb{Z},\mathbb{C}^\times)\times\mathrm{Hom}(\mathbb{Z}/m_1,\mathbb{C}^\times)\times\cdots\times\mathrm{Hom}(\mathbb{Z}/m_r,\mathbb{C}^\times) \simeq \mathbb{C}^\times \times \mathbb{G}_{m_1} \times \cdots \times \mathbb{G}_{m_r}$. □

3.4. Twisting.

There is a method, called twisting, to deform the the multiplication of a Hopf algebra [**DT**]; it is formally dual to the twisting of the comultiplication [**D, R**]. The relation with bosonization was established in [**MO**]. Here we show how to relate two cocycles over a rack X by a twisting, in a way that the corresponding Nichols algebras are preserved.

Let $\mathcal{H}$ be a Hopf algebra. Let $\phi : \mathcal{H}\otimes\mathcal{H} \to \mathbb{C}$ be an invertible (with respect to the convolution) linear map and define a new product by $x \cdot_\phi y = \phi(x_{(1)}, y_{(1)})x_{(2)}y_{(2)}\phi^{-1}(x_{(3)}, y_{(3)})$, $x, y \in \mathcal{H}$. If ϕ is a unitary 2-cocycle, that is for all $x, y, z \in \mathcal{H}$,

$$\phi(x_{(1)} \otimes y_{(1)})\,\phi(x_{(2)}y_{(2)} \otimes z) = \phi(y_{(1)} \otimes z_{(1)})\,\phi(x \otimes y_{(2)}z_{(2)}), \tag{15}$$

$$\phi(x \otimes 1) = \phi(1 \otimes x) = \varepsilon(x), \tag{16}$$

then $\mathcal{H}_\phi$ (the same coalgebra but with multiplication $\cdot_\phi$) is a Hopf algebra.

Theorem 3.8. [**MO**, 2.7, 3.4] *Let $\phi : \mathcal{H}\otimes\mathcal{H} \to \mathbb{C}$ be an invertible unitary 2-cocycle.*

(a) *There exists an equivalence of braided categories $\mathcal{T}_\phi : {}^{\mathcal{H}}_{\mathcal{H}}\mathcal{YD} \to {}^{\mathcal{H}_\phi}_{\mathcal{H}_\phi}\mathcal{YD}$, $V \mapsto V_\phi$, which is the identity on the underlying vector spaces, morphisms and coactions, and transforms the action of $\mathcal{H}$ on V to $\cdot_\phi : \mathcal{H}_\phi\otimes V_\phi \to V_\phi$,*

$$h \cdot_\phi v = \phi(h_{(1)}, v_{(-1)})(h_{(2)} \cdot v_{(0)})_{(0)}\,\phi^{-1}((h_{(2)} \cdot v_{(0)})_{(-1)}, h_{(3)}),$$

$h \in \mathcal{H}_\phi$, $v \in V_\phi$. The monoidal structure on $\mathcal{T}_\phi$ is given by the natural transformation $b_{V,W} : (V \otimes W)_\phi \to V_\phi \otimes W_\phi$

$$b_{V,W}(v \otimes w) = \phi(v_{(-1)}, w_{(-1)})v_{(0)} \otimes w_{(0)}, \quad v \in V, w \in W.$$

(b) *$\mathcal{T}_\phi$ preserves Nichols algebras: $\mathfrak{B}(V)_\phi \simeq \mathfrak{B}(V_\phi)$ as objects in ${}^{\mathcal{H}_\phi}_{\mathcal{H}_\phi}\mathcal{YD}$. In particular, the Poincaré series of $\mathfrak{B}(V)$ and $\mathfrak{B}(V_\phi)$ are the same.* □

Let us recall the argument for (b). The functor $\mathcal{T}_\phi$ preserves the braidings; that is, if c, resp. c_ϕ, is the braiding in ${}^{\mathcal{H}}_{\mathcal{H}}\mathcal{YD}$, resp. ${}^{\mathcal{H}_\phi}_{\mathcal{H}_\phi}\mathcal{YD}$, then the following diagram commutes:

$$\begin{tikzcd} (V\otimes W)_\phi \arrow[r, "\mathcal{T}_\phi(c)"] \arrow[d, "b_{V,W}"'] & (W\otimes V)_\phi \arrow[d, "b_{W,V}"] \\ V_\phi\otimes W_\phi \arrow[r, "c_\phi"] & W_\phi\otimes V_\phi. \end{tikzcd} \tag{17}$$

Since the ideal of relations of a Nichols algebra is the sum of the kernels of the various quantum symmetrizers, (b) follows immediately.

Let G be a group. If $\mathcal{H} = \mathbb{C}G$, then a unitary 2-cocycle on $\mathcal{H}$ is equivalent to a 2-cocycle $\phi \in Z^2(G, \mathbb{C}^\times)$, that is a map $\phi : G \times G \to \mathbb{C}^\times$ such that

$$\phi(g,h)\,\phi(gh,t) = \phi(h,t)\,\phi(g,ht) \tag{18}$$

and $\phi(g,e) = \phi(e,g) = 1$ for all $g,h,t \in G$.

Let $\sigma, \zeta \in G$, $\mathcal{O}_\sigma$, $\mathcal{O}_\zeta$ their conjugacy classes, $(\rho, V) \in \widehat{C_G(\sigma)}$, $(\tau, W) \in \widehat{C_G(\zeta)}$. For $\nu \in \mathcal{O}_\sigma$, $\xi \in \mathcal{O}_\zeta$, pick $g_\nu, h_\xi \in G$ such that $g_\nu \triangleright \sigma = \nu$, $h_\xi \triangleright \zeta = \xi$.

Lemma 3.9. *If $\phi \in Z^2(G, \mathbb{C}^\times)$, then the braiding*

$$c_\phi : M(\mathcal{O}_\sigma, \rho)_\phi \otimes M(\mathcal{O}_\zeta, \tau)_\phi \to M(\mathcal{O}_\zeta, \tau)_\phi \otimes M(\mathcal{O}_\sigma, \rho)_\phi$$

is given by

$$c_\phi(g_\nu v \otimes h_\xi w) = \phi(\nu, \xi)\phi^{-1}(\nu \triangleright \xi, \nu)\, \nu \cdot h_\xi w \otimes g_\nu v, \tag{19}$$

$v \in V$, $w \in W$.

Proof. By (17), since $b_{M(\mathcal{O}_\sigma,\rho),M(\mathcal{O}_\zeta,\tau)}(g_\nu v \otimes h_\xi w) = \phi(\nu,\xi)\, g_\nu v \otimes h_\xi w$. □

Let now X be a subrack of a conjugacy class $\mathcal{O}$ in G, q a 2-cocycle on X arising from some Yetter-Drinfeld module $M(\mathcal{O}, \rho)$ with $\dim \rho = 1$ and $\phi \in Z^2(G, \mathbb{C}^\times)$. Define $q^\phi : X \times X \to \mathbb{C}^\times$ by

$$q^\phi_{xy} = \phi(x,y)\phi^{-1}(x \triangleright y, x)\, q_{xy}, \quad x, y \in X. \tag{20}$$

Then Lemma 3.9 and Th. 3.8 imply that

(21) The Poincaré series of $\mathfrak{B}(X, q)$ and $\mathfrak{B}(X, q^\phi)$ are equal.

Remark 3.10. If X is any rack, q a 2-cocycle on X and $\phi : X \times X \to \mathbb{C}^\times$, then define q^ϕ by (20). It can be shown that q^ϕ is a 2-cocycle iff

$$\begin{aligned}\phi(x,z)\phi(x \triangleright y, x \triangleright z)\phi(x \triangleright (y \triangleright z), x)\phi(y \triangleright z, y)& \\ = \phi(y,z)\phi(x, y \triangleright z)\phi(x \triangleright (y \triangleright z), x \triangleright y)&\phi(x \triangleright z, x)\end{aligned} \tag{22}$$

for any $x, y, z \in X$. Thus, if X is a subrack of a group G and $\phi \in Z^2(G, \mathbb{C}^\times)$, then $\phi|_{X \times X}$ satisfies (22).

Definition 3.11. The 2-cocycles q and q' on X are *equivalent by twist* if there exists $\phi : X \times X \to \mathbb{C}^\times$ such that $q' = q^\phi$ as in (20).

4. Simple affine racks

Let p be a prime, $t \in \mathbb{N}$ and $f \in \mathbb{F}_p[\mathtt{X}]$ of degree t, monic irreducible and different from $\mathtt{X}$ and $\mathtt{X} - \mathtt{1}$. Let T be the companion matrix of f and $\mathsf{Q}_{\mathbb{F}_p^t, f} := \mathsf{Q}_{\mathbb{F}_p^t, T}$ be the associated affine rack; this will be simply denoted by Q if no emphasis is needed. Alternatively, set $q = p^t$ and identify $\mathbb{F}_q$ with $\mathbb{F}_p^t$. Then the action of T corresponds to multiplication by a, which is the class of $\mathtt{X}$ in $\mathbb{F}_p[\mathtt{X}]/(\mathtt{f})$. Note that a generates $\mathbb{F}_q$ over $\mathbb{F}_p$.

Question 5. *Find the proper subracks of* Q.

We expect that the simple affine racks will have very few subracks. In fact, they have no abelian subracks with more than one element [**AFGV1**, Remark 3.13].

Proposition 4.1. *If a generates $\mathbb{F}_q^\times$, then any proper subrack of $\mathsf{Q}_{\mathbb{F}_q,a}$ is trivial.*

Proof. Let X be a subrack of $\mathsf{Q}_{\mathbb{F}_q,a}$ with more than one element. Let $x, y \in X$ with $x \neq y$. By definition we have $\varphi_x^n(y) \in X$ for all $n \in \mathbb{N}$. Since $\varphi_x^n(y) = (1-a^n)x + a^n y$, for all $n \in \mathbb{N}$, we have that

$$A = \{(1-a^n)x + a^n y \mid 0 \leq n \leq q-1\} \subseteq X.$$

Moreover, A has q elements. Indeed, suppose there exist $m \neq n$ such that $(1-a^n)x + a^n y = (1-a^m)x + a^m y$. Then $x(a^m - a^n) = y(a^m - a^n)$ which implies that $x = y$, a contradiction. Since $A \subseteq X \subseteq \mathsf{Q}_{\mathbb{F}_q,a}$ and $|\mathsf{Q}_{\mathbb{F}_q,a}| = q$ we have that $X = \mathsf{Q}_{\mathbb{F}_q,a}$. $\square$

In the particular case $t = 1$, we can say more: any proper subrack of an affine rack with p elements is trivial.

Proposition 4.2. *Let $1 \neq a \in \mathbb{F}_p^\times$. Then any proper subrack of the affine rack $\mathsf{Q}_{\mathbb{F}_p,a}$ is trivial.*

Proof. Let $x \neq y$ be two elements of $\mathbb{F}_p$. It is enough to show that the subrack generated by x and y is $\mathbb{F}_p$. Let

$$F_{a,m}(n_1, n_2, ..., n_m) = \sum_{j=1}^{m} (-1)^{j+1} a^{n_j + \cdots + n_m}.$$

Note that $a + aF_{a,2k}(n_1, n_2, ..., n_{2k}) = F_{a,2k+1}(n_1, n_2, ..., n_{2k}, 1)$. Then

$$\varphi_y^{n_{2k}} \varphi_x^{n_{2k-1}} \cdots \varphi_x^{n_1}(y) = y + (y-x)F_{a,2k}(n_1, n_2, ..., n_{2k}), \tag{23}$$

$$\varphi_y^{n_{2k+1}} \varphi_x^{n_{2k}} \cdots \varphi_x^{n_1}(y) = x + (y-x)F_{a,2k+1}(n_1, n_2, ..., n_{2k+1}). \tag{24}$$

Let $z \in \mathbb{F}_p$, then

$$z = \varphi_y^{n_{2k}} \varphi_x^{n_{2k-1}} \cdots \varphi_x^{n_1}(y) \tag{25}$$

has at least one solution. In fact, let $n_j = (-1)^j$. Equation (23) implies that (25) can be re-written as $z = y + (y-x)(1-a)k$. Then the result follows by taking $k = (z-y)(1-a)^{-1}(y-x)^{-1}$. $\square$

5. Conjugacy classes in non-abelian simple groups

5.1. Alternating groups.

Theorem 5.1. [**AFGV1**, Th. 4.1] *Let $\sigma \in \mathbb{A}_m$, $m \geq 5$. If the type of σ is NOT any of (3^2); $(2^2, 3)$; $(1^n, 3)$; (2^4); $(1^2, 2^2)$; $(1, 2^2)$; $(1, p)$, (p) with p prime, then the conjugacy class of σ in $\mathbb{A}_m$ is of type D.* $\square$

Table 2. Conjugacy classes of sporadic groups which are not known to be of type D; those which are NOT of type D appear in bold.

G	**Classes**	G	**Classes**
M_{11}	**8A, 8B, 11A, 11B**	Co_1	3A, 23A, 23B
M_{12}	**11A, 11B**	J_1	**15A, 15B, 19A, 19B, 19C**
M_{22}	**11A, 11B**	$O'N$	31A, 31B
M_{23}	**23A, 23B**	J_3	5A, 5B, 19A, 19B
M_{24}	**23A, 23B**	Ru	29A, 29B
J_2	**2A, 3A**	He	all of type D
Suz	3A	Fi_{22}	**2A**, 22A, 22B
HS	11A, 11B	Fi_{23}	**2A**, 23A, 23B
McL	11A, 11B	HN	all of type D
Co_3	23A, 23B	Th	all of type D
Co_2	**2A**, 23A, 23B	T	2A

G	**Classes**
Ly	33A, 33B, 37A, 37B, 67A, 67B, 67C
J_4	29A, 37A, 37B, 37C, 43A, 43B, 43C
Fi'_{24}	23A, 23B, 27B, 27C, 29A, 29B, 33A, 33B, 39C, 39D
B	2A, 16C, 16D, 32A, 32B, 32C, 32D, 34A,
	46A, 46B, 47A, 47B
M	32A, 32B, 41A, 46A, 46B, 47A, 47B, 59A, 59B,
	69A, 69B, 71A, 71B, 87A, 87B, 92A, 92B, 94A, 94B

5.2. Sporadic groups.

Theorem 5.2. [**AFGV2, AFGV3**] *If G is a sporadic simple group and $\mathcal{O}$ is a non-trivial conjugacy class of G NOT listed in Table 2, then $\mathcal{O}$ is of type D.* □

5.3. Finite groups of Lie type.

Let p be a prime number, $m \in \mathbb{N}$ and $q = p^m$. Let $\mathbb{G}$ be an algebraic reductive group defined over the algebraic closure of $\mathbb{F}_q$ and $G = \mathbb{G}(\mathbb{F}_q)$ be the finite group of $\mathbb{F}_q$-points. Let $x \in G$; we want to investigate the orbit $\mathcal{O}_x^G$ of x in G. Let $x = x_s x_u$ be the Chevalley-Jordan decomposition of x in $\mathbb{G}$; then $x_s, x_u \in G$. Let $\mathbb{K} = C_{\mathbb{G}}(x_s)$, a reductive subgroup of $\mathbb{G}$ by [**Hu**, Thm. 2.2], and let $\mathbb{L}$ be its semisimple part; then $K := \mathbb{K} \cap G = C_G(x_s)$, by [**Bo**, Prop. 9.1]. Since $x_u \in K$, we conclude from Subsection 2.4 that

$$\mathcal{O}_{x_u}^K \text{ is a subrack of } \mathcal{O}_x^G.$$

Therefore, we are reduced to investigate the orbits $\mathcal{O}_x$ when x is either semisimple (the case $x = x_s$) or unipotent (by the reduction described).

The first step of the Strategy proposed in Subsection 2.6 consists of finding subracks of type D of conjugacy classes of semisimple or unipotent elements. We believe that most semisimple conjugacy classes are of type D. We give now some evidence for this belief, using techniques with involutions and elements of a Weyl group associated to a fixed $\mathbb{F}_q$-split torus.

Let $n > 1$, $\xi \in \mathbb{F}_q^\times$ so that $\operatorname{ord}\xi = m$ divides $q-1$ and $a \in \mathbb{F}_q^\times$. For all $x = (x_1, \dots, x_n) \in (\mathbb{Z}/m)^n$ such that $\sum_{i=0}^n x_i \equiv 0 \pmod m$ define n_a to be the companion matrix of the polynomial $X^n - a$, $\xi_x = \operatorname{diag}(\xi^{x_1}, \dots, \xi^{x_n})$ and $\mu_x = n_a \xi_x$.

$$\mu_x = \begin{pmatrix} 0 & & \dots & 0 & a\xi^{x_n} \\ \xi^{x_1} & 0 & \dots & 0 & 0 \\ 0 & \xi^{x_2} & \dots & 0 & \vdots \\ \vdots & & \ddots & \vdots & 0 \\ 0 & \dots & \dots & \xi^{x_{n-1}} & 0 \end{pmatrix} \in \mathbf{GL}(n, \mathbb{F}_q).$$

Let $X_{a,\xi} = \{\mu_x : \sum_{i=1}^n x_i \equiv 0 \pmod m\}$, a subset of the conjugacy class of n_a in $\mathbf{GL}(n, \mathbb{F}_q)$ (that is, the set of matrices with minimal polynomial $T^n - a$). If $a = -1$, then $X_{a,\xi} \subseteq \mathbf{SL}(n, \mathbb{F}_q)$.

The following proposition is a generalization of [**AF3**, Example 3.15].

Proposition 5.3. *Assume that $(n, q-1) \neq 1$; that $q > 3$, if $n = 4$; and that $q > 5$, if $n = 2$. Then the conjugacy class of n_a is of type D.*

Proof. Pick a generator ξ of $\mathbb{F}_q^\times$. We claim that $X_{a,\xi}$ is a subrack of the conjugacy class of n_a in $\mathbf{GL}(n, \mathbb{F}_q)$, isomorphic to the affine rack $\mathsf{Q}_{(\mathbb{Z}/(q-1))^{n-1}, g}$, with $g(x_1, \dots, x_{n-1}) = \left(-\sum_{i=1}^{n-1} x_i, x_1, \dots, x_{n-2}\right)$. A direct computation shows that $\mu_x \mu_y \mu_x^{-1} = \mu_{x \triangleright y}$, with

$$x \triangleright y = (x_1 + y_n - x_n, x_2 + y_1 - x_1, \dots, x_n + y_{n-1} - x_{n-1}).$$

Thus, the map $\varphi : X_{a,\xi} \to \mathsf{Q}_{(\mathbb{Z}/(q-1))^{n-1}, g}$ given by $\varphi(\mu_x) = (x_1, \dots, x_{n-1})$ is a rack isomorphism and the claim is proved. The proposition follows now from [**AFGaV**, Lemma 2.2], for $n > 2$, or [**AFGaV**, Lemma 2.1], for $n = 2$. $\square$

The conjugacy class of involutions in $\mathbf{PSL}(2, \mathbb{F}_q)$ for $q \in \{5, 7, 9\}$ is not of type D. For $q > 9$ we have the following result.

Corollary 5.4. (a) *Assume that $q \equiv 1 \pmod 4$ and $q > 9$. Then the conjugacy class of involutions of $\mathbf{PSL}(2, \mathbb{F}_q)$ is of type D.*

(b) *Assume that $q \equiv 3 \pmod 4$ and $q > 9$. Then the conjugacy class of involutions of $\mathbf{PGL}(2, \mathbb{F}_q)$ is of type D.*

Proof. (a) Let $\xi \in \mathbb{F}_q$ such that $\mathbb{F}_q^\times = \langle \xi \rangle$. By Proposition 5.3 with $a = -1$, the subrack $X = \{\left(\begin{smallmatrix} 0 & -\xi^{-x} \\ \xi^x & 0 \end{smallmatrix}\right) : x \in \mathbb{Z}/(q-1)\}$ of the conjugacy class of n_{-1} in $\mathbf{GL}(2, \mathbb{F}_q)$ is isomorphic to the dihedral rack $\mathcal{D}_{q-1}$. Let $\pi : \mathbf{GL}(2, \mathbb{F}_q) \to \mathbf{PGL}(2, \mathbb{F}_q)$ be the canonical projection. Then $\pi\left(\begin{smallmatrix} 0 & -\xi^{-x} \\ \xi^x & 0 \end{smallmatrix}\right) \in \mathbf{PSL}(2, \mathbb{F}_q)$ for all $x \in \mathbb{Z}/(q-1)$ and whence $\pi(X)$ is a subrack of the unique conjugacy class of involutions in $\mathbf{PSL}(2, \mathbb{F}_q)$. Now $\pi\left(\begin{smallmatrix} 0 & -\xi^{-x} \\ \xi^x & 0 \end{smallmatrix}\right) = \pi\left(\begin{smallmatrix} 0 & -\xi^{-y} \\ \xi^y & 0 \end{smallmatrix}\right)$ iff $\xi^x = -\xi^y$, hence $\pi(X) \simeq \mathcal{D}_{(q-1)/2}$, which is of type D if $(q-1)/2$ is even and > 4.

(b) Let $L = \{\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) : a, b \in \mathbb{F}_q\}$. Then L is a quadratic field extension of $\mathbb{F}_q$ and $|L| = q^2$. Consider now the group map $\det : L^\times \to \mathbb{F}_q^\times$ given by the

determinant. Since every element in a finite field is a sum of squares, the kernel is a subgroup of $L^\times$ of order $\frac{|L^\times|}{|\mathbb{F}_q^\times|} = \frac{q^2-1}{q-1}$. Since $L^\times$ is cyclic, there exist $a, b \in \mathbb{F}_q$ such that $a^2+b^2 = 1$ and $\theta = \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ generates $\ker\det$, *i.e.* it has order $q+1$. Note that, as $q \equiv 3 \pmod 4$, θ is contained in a non-split torus.

Let $n = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Then the subrack $X = \{\mu_x = n\theta^x : x \in \mathbb{Z}/(q+1)\}$ of the conjugacy class of n in $\mathbf{GL}(2, \mathbb{F}_q)$ is isomorphic to the dihedral rack $\mathcal{D}_{q+1}$. Taking π as in (a), we have that $\pi(X) \simeq \mathcal{D}_{(q+1)/2}$ is a subrack of the unique conjugacy class of involutions in $\mathbf{PGL}(2, \mathbb{F}_q)$, which is of type D if $(q+1)/2$ is even and > 4. $\square$

A similar argument as in the proof of proposition 5.3 applies with weaker hypothesis to matrices whose rational form contains n_a.

Proposition 5.5. *Let $x \in \mathbf{GL}(N, \mathbb{F}_q)$ be a semisimple element whose rational form x is $\left(\begin{smallmatrix} n_a & 0 \\ 0 & B_1 \end{smallmatrix}\right)$. Suppose there exists $B_2 \in \mathbf{GL}(N-n, \mathbb{F}_q)$ such that $B_2 \neq B_1$, $B_2 \sim B_1$ and $B_1B_2 = B_2B_1$. Then the conjugacy class of x is of type D for all $n \neq 2, 4$; or $n = 4$ and $q > 3$; or $n = 2$ and q is odd.*

Proof. Pick a generator ξ of $\mathbb{F}_q^\times$ and let μ_x be as above. Let

$$X_i = \left\{\left(\begin{smallmatrix} \mu_x & 0 \\ 0 & B_i \end{smallmatrix}\right) : \sum_{j=1}^n x_j \equiv 0 \pmod{q-1}\right\},$$

$i = 1, 2$ and $X = X_1 \coprod X_2$. Since $\left(\begin{smallmatrix} \mu_x & 0 \\ 0 & B_i \end{smallmatrix}\right) \triangleright \begin{pmatrix} \mu_y & 0 \\ 0 & B_j \end{pmatrix} = \begin{pmatrix} \mu_{x\triangleright y} & 0 \\ 0 & B_j \end{pmatrix}$ and $X_1 \cap X_2 = \emptyset$, we see that X is a decomposable rack and each X_i is isomorphic to an affine rack, by the proof of Proposition 5.3. If $x = (0, \dots, 0)$, $y = (1, 0, \dots, 0)$, $s = \left(\begin{smallmatrix} \mu_x & 0 \\ 0 & B_1 \end{smallmatrix}\right)$ and $r = \begin{pmatrix} \mu_y & 0 \\ 0 & B_2 \end{pmatrix}$, then $r \triangleright (s \triangleright (r \triangleright s)) \neq s$, by a straightforward computation, see the proof of [**AFGaV**, Lemma 2.2], whenever the prescribed restrictions on n hold. $\square$

Assume now that $\mathbb{G}$ be a Chevalley group and denote by $G = \mathbb{G}(\mathbb{F}_q)$ the group of $\mathbb{F}_q$-points. Let T be a $\mathbb{F}_q$-split torus in G and $W = N_G(T)/C_G(T)$ the corresponding Weyl group. Let $\sigma \in W$ and $n_\sigma \in N_G(T)$ be a representative of σ. Since W stabilizes T, the adjoint action of n_σ on T defines an automorphism g_σ of $(\mathbb{Z}/(q-1))^n$. Indeed, without loss of generality, we may assume that $T = \mathbb{F}_q^\times \times \cdots \times \mathbb{F}_q^\times$ and $\mathbb{F}_q^\times = \langle \xi \rangle$, with $\xi \in \mathbb{F}_q^\times$. Then for all $t \in T$, there exists $x \in (\mathbb{Z}/(q-1))^n$ such that $t = \xi_x = \operatorname{diag}(\xi^{x_1}, \dots, \xi^{x_n})$, $n = \dim T$, and the automorphism is defined by $n_\sigma \xi_x n_\sigma^{-1} = \xi_{g_\sigma(x)}$.

The following proposition is a generalization of Proposition 5.3.

Proposition 5.6. *Let $\sigma \in W$ and $n_\sigma \in N_G(T)$ be a representative of σ. Assume there exists $x \in (\mathbb{Z}/(q-1))^n$ such that $x \notin \operatorname{Im}(\operatorname{id} - g_\sigma)$ and $x - g_\sigma(x) + g_\sigma^2(x) - g_\sigma^3(x) \neq 0$. Then the conjugacy class of n_σ in G is of type D.*

Proof. Consider the set $X_{\sigma,\xi} = \{\mu_y = n_\sigma \xi_y : y \in (\mathbb{Z}/(q-1))^n\}$. Then $X_{\sigma,\xi}$ is a (non-empty) rack isomorphic to the affine rack $((\mathbb{Z}/(q-1))^n, g_\sigma)$. Indeed, since

$$\begin{aligned} \mu_x\mu_y\mu_x^{-1} &= n_\sigma\xi_x n_\sigma\xi_y\xi_x^{-1}n_\sigma^{-1} = n_\sigma\xi_x n_\sigma \xi_{y-x} n_\sigma^{-1} = n_\sigma\xi_x\xi_{g_\sigma(y-x)} \\ &= n_\sigma \xi_{g_\sigma(y)+(1-g_\sigma)(x)} = \mu_{x\triangleright y}, \end{aligned}$$

the map $\varphi : X_{\sigma,\xi} \to ((\mathbb{Z}/(q-1))^n, g_\sigma)$ given by $\varphi(\mu_x) = x$ defines a rack isomorphism. Since $x \notin \operatorname{Im}(\operatorname{id} - g_\sigma)$, $X_{\sigma,\xi}$ contains at least two cosets with respect to $\operatorname{Im}(1 - g_\sigma)$. If we take $s = \mu_0$ and $r = \mu_x$, then

$$r \triangleright (s \triangleright (r \triangleright s)) = \mu_{x \triangleright (0 \triangleright (x \triangleright 0))} = \mu_{x - g_\sigma(x) + g_\sigma^2(x) - g_\sigma^3(x)},$$

which implies that $X_{\sigma,\xi}$ is of type D. $\square$

6. Twisted conjugacy classes in simple non-abelian groups

In this section we consider twisted conjugacy classes in simple non-abelian groups defined by non-trivial outer automorphisms. These can be realized as conjugacy classes in the following way. Pick a representative of θ in $\operatorname{Aut}(L)$, called also θ, and form the semidirect product $L \rtimes \langle\theta\rangle$. Then the racks of type $(L, 1, \theta)$ are the conjugacy classes of $L \rtimes \langle\theta\rangle$ contained in $L \times \{\theta\}$.

6.1. Alternating groups.

Since $\mathbb{A}_m \rtimes \mathbb{Z}/2 \simeq \mathbb{S}_m$, the racks of this type are the conjugacy classes in $\mathbb{S}_n$ not intersecting $\mathbb{A}_n$. We keep the notation from subsection 5.1. Assume that $m \geq 5$.

Theorem 6.1. [**AFGV1**, Th. 4.1] *Let $\sigma \in \mathbb{S}_m - \mathbb{A}_m$. If the type of σ is neither $(2,3)$, nor (2^3), nor $(1^n, 2)$, then the conjugacy class of σ is of type D.* $\square$

Notice that the racks of type (2^3) and $(1^4, 2)$ are isomorphic. As we see, the only example, except for the type $(2,3)$, is $(1^n, 2)$. We treat it in the following Subsection.

6.2. The Fomin-Kirillov algebras.

Let $X = \mathcal{O}_2^m$ be the rack of transpositions in $\mathbb{S}_m$, $m \geq 3$. As shown in [**MS**], see also [**AFZ**], there are two cocycles $\mathbf{q} \in Z^2(X, \mathbb{C}^\times)$ arising from Yetter-Drinfeld modules over $\mathbb{C}\mathbb{S}_m$ and such that $\mathbf{q}_{ii} = -1$ for all (some) $i \in X$. These are either $\mathbf{q} = -1$ or $\mathbf{q} = \chi$, the cocycle given by $\chi(\sigma, \tau) = \begin{cases} 1, & \text{if } \sigma(i) < \sigma(j) \\ -1, & \text{if } \sigma(i) > \sigma(j). \end{cases}$, if τ, σ are transpositions, $\tau = (ij)$ and $i < j$. Furthermore, their classes in $Z^2(X, \mathbb{C}^\times)$ are different. Hence, we have a monomorphism $\mathbb{C}^\times \times \mathbb{G}_2 \hookrightarrow H^2(\mathcal{O}_2^m, \mathbb{C}^\times)$.

Question 6. *Is $H^2(\mathcal{O}_2^m, \mathbb{C}^\times) \simeq \mathbb{C}^\times \times \mathbb{G}_2$ for $m \geq 4$?*

We conjecture that the answer is yes; Proposition 3.7 (b) gives some computational support to this conjecture, and Proposition 3.2 should be useful for this.

We turn now to the Nichols algebras associated to $X = \mathcal{O}_2^m$.

- ◇ If $\mathbf{q} \in Z^2(X, \mathbb{C}^\times)$ arises from a Yetter-Drinfeld module over $\mathbb{C}\mathbb{S}_m$ and $\mathbf{q}_{ii} \neq -1$, then $\dim \mathfrak{B}(X, \mathbf{q}) = \infty$ [**AFZ**, Theorem 1]. In fact, assume that $m \geq 4$. Then it can be shown that $\dim \mathfrak{B}(X, \mathbf{q}) = \infty$ for any $\mathbf{q} \in \mathbb{C}^\times \times \mathbb{G}_2 \hookrightarrow H^2(\mathcal{O}_2^m, \mathbb{C}^\times)$ such that $\mathbf{q}_{ii} \neq -1$, just looking at the abelian subrack $\{(12), (34)\}$.
- ◇ The Nichols algebras $\mathfrak{B}(\mathcal{O}_2^m, -1)$ and $\mathfrak{B}(\mathcal{O}_2^m, \chi)$ are finite-dimensional for $m = 3, 4, 5$, see Table 6. Indeed, the Hilbert series of $\mathfrak{B}(\mathcal{O}_2^m, -1)$ and $\mathfrak{B}(\mathcal{O}_2^m, \chi)$ are equal.

- $\diamond$ The quadratic Nichols algebra of a braided vector space V is $\widehat{\mathfrak{B}}_2(V) = T(V)/\langle \ker Q_2\rangle$, cf. (6); clearly, here is an epimorphism $\widehat{\mathfrak{B}}_2(V) \to \mathfrak{B}(V)$. The Nichols algebras $\mathfrak{B}(\mathcal{O}_2^m, -1)$ and $\mathfrak{B}(\mathcal{O}_2^m, \chi)$ are quadratic for $m = 3, 4, 5$. Furthermore, $\mathfrak{B}(\mathcal{O}_2^m, \chi)$ appears in [**FK**] in relation with the quantum cohomology of the flag variety.
- $\diamond$ It is known if the Nichols algebras $\mathfrak{B}(\mathcal{O}_2^m, -1)$ and $\mathfrak{B}(\mathcal{O}_2^m, \chi)$ are finite-dimensional, nor if they are quadratic, for $m \geq 6$.

Question 7. *Are the cocycles -1 and χ equivalent by twist? Recall that $H^2(\mathbb{S}_m, \mathbb{C}^\times) \simeq \mathbb{Z}/2$ for $m \geq 4$, see* [**Schur**].

A positive answer to Question 7 would explain the similarities between the Nichols algebras $\mathfrak{B}(\mathcal{O}_2^m, -1)$ and $\mathfrak{B}(\mathcal{O}_2^m, \chi)$.

6.3. Sporadic groups.

The sporadic groups with non-trivial outer automorphisms group are M_{12}, M_{22}, J_2, Suz, HS, McL, He, Fi_{22}, Fi_{24}', $O'N$, J_3, T and HN. For any group L among these, the outer automorphisms group is $\mathbb{Z}/2$ and $\mathrm{Aut}(L) \simeq L \rtimes \mathbb{Z}/2$. Hence we need to consider the conjugacy classes in $\mathrm{Aut}(L) - L$.

Theorem 6.2. [**FV**] *Let G be one of the following sporadic simple groups: M_{12}, M_{22}, J_2, Suz, HS, McL, He, $O'N$, J_3 or T. If $\mathcal{O}$ is the conjugacy class of a non-trivial element in $\mathrm{Aut}(G) - G$ NOT listed in Table 3, then $\mathcal{O}$ is of type D.* $\square$

Table 3. Twisted conjugacy classes which are not known to be of type D

Group	$\mathrm{Aut}(M_{22})$	$\mathrm{Aut}(J_3)$	$\mathrm{Aut}(HS)$	$\mathrm{Aut}(McL)$	$\mathrm{Aut}(ON)$
Classes	2A	34A, 34B	2C	22A, 22B	38A, 38B, 38C

The groups $\mathrm{Aut}(Fi_{22})$, $\mathrm{Aut}(Fi_{24}')$ and $\mathrm{Aut}(HN)$ are being object of present study, see [**FV**].

7. On twisted homogeneous racks

In this section, we fix a simple non-abelian group L, an integer $t > 1$ and $\theta \in \mathrm{Out}(L)$; by abuse of notation, we call also by θ a representative in $\mathrm{Aut}(L)$. The representative of the trivial element is chosen as the trivial automorphism. Let $u \in \mathrm{Aut}(L^t)$ act by

$$u(\ell_1, \dots, \ell_t) = (\theta(\ell_t), \ell_1, \dots, \ell_{t-1}), \quad \ell_1, \dots, \ell_t \in L.$$

The twisted conjugacy class of $(x_1, \dots, x_t) \in L^t$ is called a *twisted homogeneous rack* (THR for short) of class (L, t, θ) and denoted $\mathcal{C}_{(x_1,\dots,x_t)}$. Let also $\mathcal{C}_\ell := \mathcal{C}_{(e,\dots,e,\ell)}$, $\ell \in L$. The set of twisted homogeneous racks of class (L, t, θ) is parameterized by the set of twisted conjugacy classes of L under θ [**AFGaV**, Prop. 3.3]. Namely,

(1) If $(x_1, \dots, x_t) \in L^t$ and $\ell = x_t x_{t-1} \cdots x_2 x_1$, then $\mathcal{C}_{(x_1,\dots,x_t)} = \mathcal{C}_\ell$.

(2) $\mathcal{C}_\ell = \mathcal{C}_k$ iff $k \in \mathcal{O}_\ell^{L,\theta}$; hence

$$\mathcal{C}_\ell = \{(x_1, \dots, x_t) \in L^t : \ x_t x_{t-1} \cdots x_2 x_1 \in \mathcal{O}_\ell^{L,\theta}\}.$$

In [**AFGaV**], we have developed some techniques to check whether $\mathcal{C}_\ell$ is of type D; so far, these techniques are more useful in the case $\theta = \mathrm{id}$. For illustration, we quote:

- If $\ell \in L$ is quasi-real of type j, $t \geq 3$ or $t = 2$ and $\mathrm{ord}(\ell) \nmid 2(1-j)$, then $\mathcal{C}_\ell$ is of type D.
- If ℓ is an involution and $t > 4$ is even, then $\mathcal{C}_\ell$ is of type D.
- If ℓ is an involution, t is odd and $\mathcal{O}_\ell^L$ is of type D, then so is $\mathcal{C}_\ell$.
- If $(t, |L|)$ is divisible by an odd prime p, or if $(t, |L|)$ is divisible by $p = 2$ and $t \geq 6$, then $\mathcal{C}_e$ is of type D.
- If $L = \mathbb{A}_5$ or $\mathbb{A}_6$ and $t = 2$, then $\mathcal{C}_e$ is not of type D (checked with GAP).

In other words, at least when $\theta = \mathrm{id}$, the worse cases are either when ℓ is an involution and $t = 2, 4$, or else when $\ell = e$.

As an application of these techniques, we have the following result.

Theorem 7.1. [**AFGaV**] *Let L be $\mathbb{A}_n$, $n \geq 5$, or a sporadic group, $t \geq 2$ and $\ell \in L$. If $\mathcal{C}_\ell$ is a twisted homogeneous rack of class (L, t, id) not listed in Tables 4 and 5, then $\mathcal{C}_\ell$ is of type D.* □

Table 4. THR $\mathcal{C}_\ell$ of type $(\mathbb{A}_n, t, \theta)$, $\theta = \mathrm{id}$, $t \geq 2$, $n \geq 5$, which are not known to be of type D. Those not of type D are in bold.

n	ℓ	Type of ℓ	t
any	e	(1^n)	odd, $(t, n!) = 1$
5		$(\mathbf{1^5})$	$\mathbf{2}$
5		(1^5)	4
6		$(\mathbf{1^6})$	$\mathbf{2}$
5	involution	$(1, 2^2)$	4, odd
6		$(1^2, 2^2)$	odd
8		(2^4)	odd
any	order 4	$(1^{r_1}, 2^{r_2}, 4^{r_4})$, $r_4 > 0$, $r_2 + r_4$ even	2

Table 5. THR $\mathcal{C}_\ell$ of type (L, t, θ), with L a sporadic group, $\theta = \mathrm{id}$, which are not known to be of type D.

sporadic	t	**Type of ℓ or class name of $\mathcal{O}_\ell^L$**
any	$(t, \lvert L\rvert) = 1$, t odd	1A
	2	$\mathrm{ord}(\ell) = 4$
T, J_2, Fi_{22}, Fi_{23}, Co_2	odd	2A
B	odd	2A, 2C
Suz	any	6B, 6C

8. Applications to the classification of pointed Hopf algebras

We say that a finite group G *collapses* if for any finite-dimensional pointed Hopf algebra H, with $G(H) \simeq G$, necessarily $H \simeq \mathbb{C}G$. Some applications of the results on Nichols algebras presented here to the classification of Hopf algebras need the following Lemma.

Lemma 8.1. [**AFGV1**, Lemma 1.4] *The following statements are equivalent:*

(1) *If* $0 \neq V \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$, *then* $\dim \mathfrak{B}(V) = \infty$.
(2) *If* $V \in {}^{\mathbb{C}G}_{\mathbb{C}G}\mathcal{YD}$ *is* irreducible, *then* $\dim \mathfrak{B}(V) = \infty$.
(3) *G collapses.* □

Theorem 8.2. [**AFGV1, AFGV2**] *Let G be either an alternating group $\mathbb{A}_m$, $m \geq 5$, or a sporadic simple group, different from the Fischer group Fi_{22}, the Baby Monster B and the Monster M. Then G collapses.* □

The proof goes as follows: by the Lemma 8.1, we need to show that $\dim \mathfrak{B}(V) = \infty$ for any irreducible $V = M(\mathcal{O}, \rho)$. If $\mathcal{O}$ is of type D, this follows from Theorem 2.4; and we know those classes of type D by Theorems 5.1, 5.2. The remaining pairs $(\mathcal{O}, \rho)$ are treated by abelian techniques, namely one finds an abelian subrack, computes the corresponding diagonal braiding arising from ρ and applies [**H2**].

However, there are finite non-abelian groups that do not collapse. Furthermore, the classification of all finite-dimensional pointed Hopf algebras with group G is known, when $G = \mathbb{S}_3$, $\mathbb{S}_4$ or $\mathbb{D}_{4t}$, $t \geq 3$, see [**AHS, GG, FG**], respectively.

Appendix A. Examples of finite-dimensional Nichols algebras

Table 6 contains several examples of pairs $(X, \mathbf{q})$ such that $\dim \mathfrak{B}(X, \mathbf{q}) < \infty$; we give the dimension, the top degree and the reference where the example appeared[3].

Appendix B. Questions

Question 1. *Determine all simple racks of type D.*

Question 2. *For any finite indecomposable rack X, for any $n \in \mathbb{N}$, and for any $\mathbf{q} \in H^2(X, \mathbf{GL}(n, \mathbb{C}))$, determine if $\dim \mathfrak{B}(X, \mathbf{q}) < \infty$.*

Question 3. *If X collapses at 1, does necessarily X collapse?*

Question 4. *Compute all cocycles $\mathbf{q} \in Z^2(X, \mathbb{C}^\times)$ such that $\mathbf{q}_{ii} = -1$.*

Question 5. *Is $H^2(\mathcal{O}_2^m, \mathbb{C}^\times) \simeq \mathbb{C}^\times \times \mathbb{G}_2$ for $m \geq 4$?*

Question 6. *Find the proper subracks of* Q.

[3] The Nichols algebra corresponding to $\mathsf{Q}_{\mathbb{Z}/5,2}$ was actually computed by Matías Graña. The quadratic Nichols algebra corresponding to $\mathcal{O}_2^5$ was computed by Jan-Erik Roos; Graña showed that this is a Nichols algebra. The computation of the Nichols algebras corresponding to $(\mathcal{O}_2^n, \chi)$, $n = 4, 5$, was done in [**GG**] using Deriva with the help of M. Graña.

TABLE 6. Finite-dimensional $\mathfrak{B}(X, \mathbf{q})$

X	**rk**	**q**	**Relations**	$\dim \mathfrak{B}(V)$	**top**	**Ref.**
$\mathcal{D}_3$	3	-1	5 in degree 2	$12 = 3.2^2$	$4 = 2^2$	[**MS**]
$\mathcal{T}$	4	-1	8 in degree 2, 1 in degree 6	72	$9 = 3^2$	[**G1**]
$\mathsf{Q}_{\mathbb{Z}/5,2}$	5	-1	10 in degree 2, 1 in degree 4	$1280 = 5.4^4$	$16 = 4^2$	[**AG**]
$\mathsf{Q}_{\mathbb{Z}/5,3}$	5	-1	10 in degree 2, 1 in degree 4	$1280 = 5.4^4$	$16 = 4^2$	dual of the preceding
$\mathcal{O}_2^4$	6	-1	16 in degree 2	$576 = 24^3$	12	[**FK, MS**]
$\mathcal{O}_2^4$	6	χ	16 in degree 2	$576 = 24^3$	12	[**GG**]
$\mathcal{O}_4^4$	6	-1	16 in degree 2	$576 = 24^3$	12	[**AG**]
$\mathsf{Q}_{\mathbb{Z}/7,3}$	7	-1	21 in degree 2, 1 in degree 6	$326592 = 7.6^6$	$36 = 6^2$	[**G2**]
$\mathsf{Q}_{\mathbb{Z}/7,5}$	7	-1	21 in degree 2, 1 in degree 6	$326592 = 7.6^6$	$36 = 6^2$	dual of the preceding
$\mathcal{O}_2^5$	10	-1	45 in degree 2	8294400	40	[**FK, G2**]
$\mathcal{O}_2^5$	10	χ	45 in degree 2	8294400	40	[**GG**]

Question 7. *Are the cocycles -1 and χ equivalent by twist? Recall that $H^2(\mathbb{S}_m, \mathbb{C}^\times) \simeq \mathbb{Z}/2$ for $m \geq 4$, see* [**Schur**].

Acknowledgements. N. A., G. A. G. and L. V. want to thank the Organizing Committee the invitation to attend to the *XVIII Coloquio Latinoamericano de Álgebra* and the warm hospitality in São Pedro during the Colloquium. Specially, G. A. G. thanks the invitation to give the mini-curse "Quantum Groups and Hopf Algebras".

References

[A] N. Andruskiewitsch, *About finite dimensional Hopf algebras*, Notes of a course given at the CIMPA School "Quantum symmetries in theoretical physics and mathematics", Bariloche 2000. Contemp. Math **2**94 (2002), 1–57.

[AF1] N. Andruskiewitsch and F. Fantino, *On pointed Hopf algebras associated with unmixed conjugacy classes in $\mathbb{S}_m$*, J. Math. Phys. **48** (2007), 033502-1–26.

[AF2] ———, *On pointed Hopf algebras associated with alternating and dihedral groups*, Rev. Unión Mat. Argent. **48-3** (2007), 57–71.

[AF3] ———, *New techniques for pointed Hopf algebras*, Contemp. Math. 491 (2009), 323-348.

[AFGV1] N. Andruskiewitsch, F. Fantino, M. Graña and L. Vendramin, *Finite-dimensional pointed Hopf algebras with alternating groups are trivial*. arXiv:0812.4628, Ann. Mat. Pura Appl. (4), to appear.

[AFGV2] ———, *Pointed Hopf algebras over the sporadic groups*. arXiv:1001.1108, submitted.

[AFGV3] ———, *The logbook of pointed Hopf algebras over the sporadic simple groups*. arXiv:1001.1113, submitted.

[AFGaV] N. Andruskiewitsch, F. Fantino, G. A. García and L. Vendramin, *On Twisted homogeneous racks of type D*, submitted.

[AFZ] N. Andruskiewitsch, F. Fantino and S. Zhang, *On pointed Hopf algebras associated with the symmetric groups*, Manuscripta Math. **128** (2009), 359–371.

[AG] N. Andruskiewitsch and M. Graña, *From racks to pointed Hopf algebras*, Adv. Math. **178** (2003), 177 – 243.

[AHS] N. Andruskiewitsch, I. Heckenberger and H.-J. Schneider, *The Nichols algebra of a semisimple Yetter-Drinfeld module*, Amer. J. Math., to appear.

[AS1] N. Andruskiewitsch and H.-J. Schneider, *Finite quantum groups and Cartan matrices*. Adv. Math **54** (2000), 1–45.

[AS2] ———, *Pointed Hopf Algebras*, in "New directions in Hopf algebras", 1–68, Math. Sci. Res. Inst. Publ. **43**, Cambridge Univ. Press, 2002.

[AS3] ———, *On the classification of finite-dimensional pointed Hopf algebras*, Ann. Math. **171** (2010), 375–417.

[AZ] N. Andruskiewitsch and S. Zhang, *On pointed Hopf algebras associated to some conjugacy classes in $\mathbb{S}_n$*, Proc. Amer. Math. Soc. **135** (2007), no. 9, 2723–2731.

[Ang] I. Angiono, *On Nichols algebras with standard braiding*, Algebra and Number Theory Vol. 3, No. **1** (2009), 35-106.

[Ar] E. Artin, *Theory of braids*, Ann. Math. **48** (1947), 101–126.

[Bi] J. S. Birman, *Braids, links and mapping class groups*, Princeton Univ. Press (1975).

[Bo] A. Borel, *Linear algebraic groups*, Second edition, Graduate Texts in Mathematics, **126**, Springer-Verlag, New York, 1991. xii+288 pp.

[B] N. Bourbaki, *Groupes et algèbres de Lie Chap. IV, V, VI*, Hermann, Paris, 1968.

[Bk] E. Brieskorn, *Automorphic sets and singularities*, Contemp. Math. **78** (1988), 45–115.

[DT] Y. Doi and M. Takeuchi, *Multiplication alteration by two-cocycles. The quantum version*, Commun. Algebra **22**, No.14 (1994), 5715-5732.

[D] V. Drinfeld, *Quasi-Hopf algebras*, Leningrad Math. J. **1** (1990), 1419–1457.

[EGñ] P. Etingof and M. Graña, *On rack cohomology*, J. of Pure and Applied Algebra, **177** (2003), 49–59.

[ESS] P. Etingof, T. Schedler and A. Soloviev, *Set-theoretical solutions to the Quantum Yang–Baxter Equation*, Duke Math. J. **100** (1999), 169–209.

[F] F. Fantino, *On pointed Hopf algebras associated with Mathieu groups*, J. Algebra Appl. **8** 5 (2009) 633–672.

[FG] F. Fantino and G. A. García, *On pointed Hopf algebras over dihedral groups*. preprint:\protect\vrule width0pt\protect\href{http://arxiv.org/abs/1007.0227}{arXiv:1007.0227}.

[FV] F. Fantino and L. Vendramin, *On twisted conjugacy classes in sporadic groups of type D*. In preparation.

[FR] R. Fenn and C. Rourke, *Racks and links in codimension two*, J. Knot Theory Ramifications **1** 4 (1992), 343–406.

[FK] S. Fomin and K. N. Kirillov, *Quadratic algebras, Dunkl elements, and Schubert calculus*, Progr. Math. **172**, Birkhauser, (1999), 146–182.

[FGV1] S. Freyre, M. Graña and L. Vendramin, *On Nichols algebras over* $\mathbf{GL}(2,\mathbb{F}_q)$ *and* $\mathbf{SL}(2,\mathbb{F}_q)$, J. Math. Phys. **48** (2007), 123513-1 – 123513-11.

[FGV2] ______, *On Nichols algebras over* $\mathbf{PSL}(2,q)$ *and* $\mathbf{PGL}(2,q)$, J. Algebra Appl., Vol. 9, No. 2 (2010), 195–208.

[GAP] The GAP Group. GAP – Groups, Algorithms, and Programming, version 4.4.12, `http://www.gap-system.org`, 2008.

[GG] G. A. García and A. García Iglesias, *Finite dimensional pointed Hopf algebras over* $\mathbb{S}_4$, Israel Journal of Math., to appear, preprint: `arXiv:0904.2558v2`.

[G1] M. Graña, *On Nichols algebras of low dimension*, in "New Trends in Hopf Algebra Theory"; Contemp. Math. **267** (2000), 111–136.

[G2] ______, Finite dimensional Nichols algebras of non-diagonal group type, zoo of examples available at `\protect\vrule`width0pthttp://mate.dm.uba.ar/∼matiasg/zoo.html .

[GHV] M. Graña, I. Heckenberger and L. Vendramin, *Nichols algebras of group type with many quadratic relations*, preprint: `arXiv:1004.3723v1`.

[GV] M. Graña and L. Vendramin, *RiG, A* GAP *package for racks and Nichols Algebras*, available at `http://mate.dm.uba.ar/~lvendram`.

[H1] I. Heckenberger, *The Weyl groupoid of a Nichols algebra of diagonal type*, Invent. Math. **164** (2006), 175–188.

[H2] ______, *Classification of arithmetic root systems*, Adv. Math. **220** (2009), 59–124.

[HS] I. Heckenberger and H.-J. Schneider, *Root systems and Weyl groupoids for semisimple Nichols algebras*, `arXiv:0807.0691`. Proc. London Math. Soc., to appear.

[Hu] J.E. Humphreys, *Conjugacy classes in semisimple algebraic groups*, Mathematical Surveys and Monographs, **43**, American Mathematical Society, Providence, RI, 1995. xviii+196 pp.

[J] D. Joyce, *Simple quandles*, J. Algebra **79** 2 (1982), 307–318.

[LYZ] J.-H. Lu, M. Yan & Y. Zhu, *On Set-theoretical Yang–Baxter equation*, Duke Math. J. **104** (2000), 1–18.

[MO] S. Majid and R. Oeckl, *Twisting of Quantum Differentials and the Planck Scale Hopf Algebra*, Commun. Math. Phys. **205** (1999), 617–655.

[MS] A. Milinski and H-J. H.-J. Schneider, *Pointed Indecomposable Hopf Algebras over Coxeter Groups*, Contemp. Math. **267** (2000), 215–236.

[R] N. Reshetikhin, *Multiparameter quantum groups and twisted quasitriangular Hopf algebras*, Lett. Math. Phys. **2**0, (1990), pp. 331–335.

[Schur] I. Schur, *Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen*, Journal für die reine und angewandte Mathematik **139**, 155–250.

[S] A. Soloviev, *Non-unitary set-theoretical solutions to the quantum Yang–Baxter equation*, Math. Res. Lett. **7** (2000), no. 5-6, pp. 577–596.

[Tk] M. Takeuchi, *Survey of braided Hopf algebras*, in "New Trends in Hopf Algebra Theory"; Contemp. Math. **267** (2000), 301–324.

N. A., F. F., G. A. G.: Facultad de Matemática, Astronomía y Física, Universidad Nacional de Córdoba. CIEM – CONICET. Medina Allende s/n (5000), Ciudad Universitaria, Córdoba, Argentina

F. F., G. A. G.: Facultad de Ciencias Exactas, Físicas y Naturales, Universidad Nacional de Córdoba. Velez Sarsfield 1611 (5000), Ciudad Universitaria, Córdoba, Argentina

L. V. : Departamento de Matemática, FCEyN, Universidad de Buenos Aires, Pab. I, Ciudad Universitaria (1428), Buenos Aires, Argentina

L. V. : Instituto de Ciencias, Universidad de Gral. Sarmiento, J.M. Gutierrez 1150, Los Polvorines (1653), Buenos Aires, Argentina

E-mail address: `(andrus, fantino, ggarcia)@famaf.unc.edu.ar`

E-mail address: `lvendramin@dm.uba.ar`